Deloitte.

Forvaltningsrevisjon | Bergen kommune

Informasjonssikkerhet i skolesektoren

Desember 2019

«Forvaltningsrevisjon av informasjonssikkerhet i skolesektoren»

Desember 2019

Rapporten er utarbeidet for Bergen kommune av Deloitte AS.

Deloitte AS
Postboks 6013 Postterminalen,
5892 Bergen
tlf: 55 21 81 00
www.deloitte.no
forvaltningsrevisjon@deloitte.no

Sammendrag

Deloitte har i samsvar med bestilling fra kontrollutvalget i Bergen kommune gjennomført en forvaltningsrevisjon av informasjonssikkerhet i skolesektoren i kommunen. Formålet med forvaltningsrevisjonen har vært å undersøke hvordan informasjonssikkerheten er ivaretatt i skolesektoren i Bergen kommune. Fokuset i forvaltningsrevisjonen har vært på etterlevelse av kommunens styringssystem for informasjonssikkerhet.

Som datagrunnlag har revisjonen benyttet dokumentanalyse, intervju, spørreundersøkelser, tekniske sikkerhetstester og nettfiskeforsøk. Forvaltningsrevisjonen er gjennomført fra februar til desember 2019.

Rutiner og ansvar for informasjonssikkerhet

Gjennom styringssystemet for personvern og informasjonssikkerhet og tilhørende oppdragsbeskrivelser, mandater og veiledere, har Bergen kommune skriftliggjort ansvar og oppgaver knyttet til informasjonssikkerhet.

Undersøkelsen viser imidlertid at rolle- og ansvarsfordelingen knyttet til informasjonssikkerhet i skolesektoren verken oppleves som tydelig eller som hensiktsmessig organisert. Informasjonssikkerhetsarbeidet sentralt i skolesektoren i Bergen kommune preges av en uformell rolle- og ansvarsdeling, noe som gir økt risiko for uklarheter og manglende oppfølging av informasjonssikkerhetsarbeide, med tilhørende risiko for brudd på informasjonssikkerheten. Revisjonen mener at informasjonssikkerhetsbruddet høsten 2019 viser at slik risiko har gjort seg gjeldende i kommunen.

Videre viser undersøkelsen at det ute i skolene ikke er etablert klare rutiner og ansvarsforhold med hensyn til informasjonssikkerhet. I tillegg kommer det frem at det som er etablert av rutiner og ansvarsforhold er delvis avvikende fra kommunens styringssystem for informasjonssikkerhet. Funn i undersøkelsen viser også at roller og ansvar knyttet til informasjonssikkerhet blir oppfatte som uklart for en relativt stor andel av rektorene ved skolene, samt at informasjonssikkerhetsoppgaver som påhviler rektorene bare delvis blir gjennomført.

Revisjonen er oppmerksom på at det er relativt kort tid siden gjeldende styringssystem for personvern og informasjonssikkerhet ble utarbeidet og implementert i kommunen, og videre at byrådsavdelingen nylig er omorganisert. Dette er begge momenter som kan være med å forklare at rutiner og ansvarsforhold i skolesektoren når det gjelder informasjonssikkerhet ikke fremstår som entydige eller klare. Revisjonen ser det i den sammenheng som positivt at det er opprettet en stilling som informasjonssikkerhetsrådgiver i skolesektoren,[1] at det er etablert en seksjon for HR, digitalisering og virksomhetsstyring som blant annet skal arbeide med å ivareta IKT-sikkerheten i byrådsavdelingen og skolesektoren, og at områdelederne i ny organisering er tiltenkt en rolle for å legge til rette for at skolene etterlever styringssystemet for informasjonssikkerhet og personvern.

Konfidensialitet

Bergen kommune har formalisert ansvar og oppgaver knyttet til å **hindre uautorisert innsyn i konfidensielle opplysninger** gjennom styringssystemet for personvern og informasjonssikkerhet med tilhørende dokumenter.

Informasjonssikkerhetsbruddet knyttet til innsyn i konfidensielle opplysninger i forbindelse med implementeringen av Vigilo, tyder på at verken system, rutiner eller ansvars- og oppgavefordeling for å hindre uautorisert innsyn i konfidensielle opplysninger er tilstrekkelig ivaretatt i skolesektoren i Bergen kommune.

Det er nylig implementert tekniske tiltak (to-faktorautentisering) som bidrar til å hindre uautorisert innsyn i konfidensielle opplysninger i systemer i skolesektoren hvor det lagres visse typer opplysninger om elever.

[1] Stillingen var på revisjonstidspunktet ikke besatt, men kommunen viser til at de har leid inn ekstern hjelp med relevant kompetanse fra januar 2019 for å arbeide på dette feltet.

Det er imidlertid mulig å omgå disse for flere av systemene som er i bruk i skolesektoren. Det er pågående prosesser for å utbedre sikkerhetshullene, men på revisjonstidspunktet var ikke disse ferdigstilte.

Når det gjelder skolenes praksis for å hindre uautorisert innsyn i konfidensielle opplysninger i skolesektoren, viser svarene i spørreundersøkelsene at det er en til dels vesentlig risiko for brudd på konfidensialiteten i skolesektoren; om lag én av fem svarer 21 % at de enten har delt passordet sitt med IT-avdelingen eller andre, noe som bryter med grunnleggende informasjonssikkerhetsprinsipper. Svarene i spørreundersøkelsen viser videre at det både forekommer at dokumenter med personopplysninger eller annen fortrolig informasjon blir oppbevart i ulåste skuffer eller hyller, at denne typen papirdokument oppbevares lett tilgjengelig, og at ansatte tar med seg konfidensielle papirdokument hjem. Også slik praksis utgjør vesentlig risiko for brudd på konfidensialiteten.

Bergen kommune har etablert noen rutiner og retningslinjer for **lagring av konfidensielle opplysninger**. Noen av retningslinjene ser imidlertid ikke ut til å være en integrert del av i kommunens styringssystem for personvern og informasjonssikkerhet, og det kommer frem av undersøkelsen at de heller ikke er kjente for sentrale ansatte når det gjelder systemsikkerhet i skolesektoren. Det er ikke tilfredsstillende at det som eksisterer av utfyllende retningslinjer knyttet til sikker lagring av konfidensielle opplysninger verken er kjent eller inngår i styringssystemet for informasjonssikkerhet. Dette gir økt sannsynlighet for feil og slik også risiko for at konfidensiell informasjon lagres uten tilstrekkelig sikring.

Revisjonen vurderer ellers at det i skolesektoren bare delvis er etablert rutiner og praksis for sikring av konfidensialitet med hensyn til bruk av sikker sone for lagring av konfidensielle opplysninger.

Bergen kommune har prosedyrer, rutiner og retningslinjer som stiller krav til **kryptering av konfidensielle opplysninger**. Både i oppdragsbeskrivelser, sjekklister og mer detaljert veiledningsmateriell går det frem hvilke typer opplysninger og informasjon som skal krypteres. Funn i undersøkelsen tyder imidlertid på det i skolesektoren bare delvis er en etablert praksis å kryptere konfidensielle opplysninger.

Tilgangsstyring

Kommunens styringssystem for personvern og informasjonssikkerhet plasserer ansvaret og de overordne oppgavene for å hindre uautorisert tilgang til informasjonssystemene. Det er i tilhørende dokument også nedfelt noen overordnede rutiner, regler og instrukser for å hindre uautorisert tilgang til informasjonssystemene.

Funn i undersøkelsen tyder på at det i de større systemene eid av skolesektoren er relativt lav risiko for at uautoriserte får tilgang, mens risikoen for dette er høyere i de mindre, pedagogiske systemene.

De gjennomførte sikkerhetstestene av kommunens IKT-systemer og fagsystemet *itslearning* avdekket ingen kritiske sårbarheter. Det ble imidlertid identifisert sårbarheter med både høy, moderat og lav risiko. Disse medfører risiko for brudd på informasjonssikkerheten i informasjonssystemene som blir benyttet i skolesektoren.

Kommunens system og rutiner for tilgangsstyring er ellers bare i noen grad egnet til sikre at ansatte får tilgangene de trenger når de trenger dem, og for å sikre at ansatte som slutter i kommunen mister tilgangene sine. Funn i undersøkelsen tyder på at det er en viss risiko for at ansatte ikke har tilganger de trenger, og en noe større risiko for at ansatte har tilganger de ikke har tjenstlig behov for.

Undersøkelsen viser også at praksis knyttet til vurdering av riktige tilganger ikke er tilstrekkelig innarbeidet i organisasjonen; nesten én av fire rektorer som deltok i spørreundersøkelsen svarer at det ikke er, eller at de ikke vet om det er, praksis knyttet til jevnlig vurdering av riktige tilganger. Dette er ikke tilfredsstillende all den tid det er rektorene som er ansvarlige for å melde videre behovet for endringer i tilgangene til informasjonssystemene.

For noen av de større systemene er det mulig å få oversikt over hvilke brukere som logger seg på. Det fremgår ikke i undersøkelsen om denne muligheten benyttes systematisk i skolenes informasjonssikkerhetsarbeid. Det er ikke mulig å loggføre brukte tilganger i de mindre systemene, noe som gjør at det ikke er mulig å avdekke eventuelle uautorisert tilganger i disse systemene. Skolesektoren i Bergen

kommune har slik ikke tilstrekkelig oversikt over hvem som behandler informasjon i informasjons-systemene.

Opplæring og kompetanse

Bergen kommune har lagt til rette for at ansatte kan tilegne seg kunnskap og kompetanse knyttet til informasjonssikkerhet og personvern, gjennom blant annet plassering av opplæringsansvar og tilgjengeliggjøring av veiledningsmateriell. Svarene i spørreundersøkelsen indikerer imidlertid at en relativt stor del av rektorene bare delvis oppgir å ha besørget nødvendig opplæring for sine ansatte knyttet til informasjonssikkerhet. Dette reflekteres i svar fra ansatte i skolesektoren på spørsmål om mottatt opplæring, der over halvparten av respondentene oppgir å ikke ha fått tilstrekkelig opplæring knyttet til personvern og informasjonssikkerhet.

Revisjonen er oppmerksom på at gjeldende styringssystem for informasjonssikkerhet relativt nylig ble utarbeidet og implementert, og videre at det er planer om å tilby de ansatte ytterligere opplæring. Likevel er det revisjonen sin vurdering at kommunen ikke fullt ut er i samsvar med krav og anbefalinger om å sikre tilstrekkelig informasjonssikkerhetskompetanse blant de ansatte i skolesektoren gjennom opplæringstiltak. Dette medfører økt sannsynlighet for at de ansatte i skolesektoren ikke har tilstrekkelig kompetanse innen informasjonssikkerhet, noe som øker risikoen for brudd på regelverket som gjelder for behandling av personopplysninger og for informasjonssikkerhet generelt. Funnene i undersøkelsen knyttet til informasjonssikkerhetskompetanse og –praksis tyder videre på at denne risikoen har gjort seg gjeldende i skolesektoren.

Revisjonen sine anbefalinger fremgår i kapittel 7

Innhold

Detaljert innholdsfortegnelse

Figurer

Tabeller

1. Innledning

1.1 Bakgrunn

Deloitte har gjennomført en forvaltningsrevisjon av informasjonssikkerhet i skolesektoren i Bergen kommune. Prosjektet ble bestilt av kontrollutvalget i Bergen kommune i sak 88/18, 18. desember 2018.[2]

1.2 Formål og problemstillinger

Formålet med forvaltningsrevisjonen har vært å undersøke hvordan informasjonssikkerheten er ivaretatt i skolesektoren i Bergen kommune. Fokuset i forvaltningsrevisjonen har vært på etterlevelse av kommunens styringssystem for informasjonssikkerhet.

Med bakgrunn i formålet har følgende problemstillinger blitt undersøkt:

1) Har skolesektoren etablert klare rutiner og ansvarsforhold med hensyn til informasjonssikkerhet i samsvar med kommunens styringssystem for informasjonssikkerhet?

2) Har skolesektoren etablert rutiner for sikring av konfidensialitet, og etterleves disse? Under dette:

   a) Hindre uautorisert innsyn i konfidensielle opplysninger
   b) Sikker sone for lagring av konfidensielle opplysninger
   c) Kryptering av konfidensielle opplysninger

3) Har skolesektoren etablert rutiner for tilgangsstyring, og etterleves disse? Under dette:

   a) Hindring av uautorisert tilgang til informasjonssystemene
   b) Inn- og utmelding av ansatte i relevante informasjonssystemene
   c) Vurdering av om ansatte har riktige tilganger i informasjonssystemene
   d) Loggføring av brukte tilganger i informasjonssystemene

4) I hvilken grad har de ansatte i skolesektoren kjennskap til retningslinjer og rutiner for informasjonssikkerhet?

1.3 Avgrensning

Revisjonen har fokusert på de krav som er stilt til informasjonssikkerhet knyttet til personopplysninger (personopplysningssikkerhet). På dette området er det stilt strenge krav, og brudd på personopplysningssikkerheten kan få store konsekvenser, både for kommunen og enkeltmennesker. Gjennomgangen omfatter også informasjonssikkerhet knyttet til annen informasjon, som sensitive opplysninger og fortrolige opplysninger.

1.4 Metode

Oppdraget er utført i samsvar med gjeldende standard for forvaltningsrevisjon (RSK 001) og kvalitetssikring er underlagt kravene til kvalitetssikring i Deloitte Policy Manual (DPM).

Oppdraget er gjennomført i tidsrommet februar 2019 til desember 2019.

1.4.1 Dokumentanalyse

Rettsregler og kommunale vedtak har blitt gjennomgått og benyttet som revisjonskriterier. Videre har revisjonen gjennomgått Bergen kommune sitt styringssystem for informasjonssikkerhet og annen relevant dokumentasjon knyttet til informasjonssikkerhet, og vurdert dette opp mot revisjonskriteriene.

[2] Prosjektet ble bestilt og var i all hovedsak gjennomført før informasjonssikkerhetsbruddet knyttet til Vigilo inntraff og ble kjent.

1.4.2 Intervju

For å få supplerende informasjon til de skriftlige kildene, har Deloitte intervjuet utvalgte personer i Bergen kommune som er involvert i arbeidet med informasjonssikkerhet og har et særskilt ansvar knyttet til systemsikkerhet. Revisjonen har intervjuet fire personer; IKT-koordinator, pedagogisk IKT-koordinator og to systemkoordinatorer.[3]

1.4.3 Spørreundersøkelse

Revisjonen har gjennomført to spørreundersøkelser; én ble sendt til et utvalg ansatte i skolene i Bergen kommune, og én ble sendt til alle rektorene i kommunens skoler.

Spørreundersøkelsen blant de ansatte ble gjennomført i forbindelse med forvaltningsrevisjonen av overordnet informasjonssikkerhet i Bergen kommune. Formålet med undersøkelsen var å kartlegge kjennskap og holdning til informasjonssikkerhet blant de ansatte.[4] Revisjonen har skilt ut svarene fra de ansatte i skolesektoren i denne spørreundersøkelsen, og det er disse som blir gjengitt i rapporten.

I undersøkelsen som gikk til rektorene var spørsmålene rettet spesifikt mot hvordan disse ivaretar sitt informasjonssikkerhetsansvar som resultatenhetsledere, samt deres egne vurderinger av risiko knyttet til informasjonssikkerhet på skolen.

Tabell 1: Svarprosent per spørreundersøkelse

Respondentgruppe	Inviterte	Besvarte	Svarprosent
Ansatte i skolen	331	120	36 %
Rektorer[5]	85	62	73 %

1.4.4 Sikkerhetstester

Revisjonen har gjennomført sikkerhetstester i ulike deler av kommunens IKT-system, samt av et fagsystem brukt i skolesektoren. Formålet med testene har vært å undersøke, kartlegge og identifisere eventuelle sårbarheter i IKT-systemene og det aktuelle fagsystemet som ved utnyttelse svekker konfidensialiteten, integriteten og/eller tilgangen til kommunens infrastruktur og/eller data.

I sikkerhetstestene av kommunens IKT-systemer undersøkte revisjonen om og hvordan kommunen i praksis ivaretar den tekniske informasjonssikkerheten. Disse sikkerhetstestene ble gjennomført også som del av forvaltningsrevisjonen av overordnet informasjonssikkerhet i Bergen kommune. Testene fokuserte både på eksterne og interne deler av kommunens systemer.[6] Ikke alle delene av testene er relevante for denne forvaltningsrevisjonen. For undersøkelsene knyttet til skolesektoren, er det den interne sikkerhetstesten som er relevant. Denne ble gjennomført via fjerntilgang til tre fysiske maskiner som stod i kommunens interne nettverk.[7] Fokuset for testen var å avdekke hvorvidt eksisterende sikkerhetskontroller og/eller filtreringsmekanismer forhindrer uautorisert tilgang til tjenester og tilgrensende nettverk. Sikkerhetsvurderingen ble gjennomført i form av en penetrasjonstest hvor det ble gjort flere tjeneste- og sårbarhetsskanninger med formål å kartlegge eksponerte tjenere og tjenester, og eventuelle sårbarheter i de identifiserte tjenestene. Videre ble det gjort forsøk på ulike tilnærminger for å omgå eksisterende sikkerhetsmekanismer.

---

[3] Alle de intervjuede var på intervjutidspunktet ansatt i seksjon skole i BBSI. Etter omorganiseringen arbeider intervjuobjektene henholdsvis i etat for skole og seksjon for HR, digitalisering og virksomhetsstyring i BBSI.
[4] Utelukket fra utvalget var ansatte som jobber i kommunalt AS, politikere, ansatte med stillingsprosent under 40 %, ekstrahjelper, vikarer, o.l., samt stillingstypene assistenter, renholdere, studenter og pensjonister.
[5] Seks skoler hadde avdelingsledere som stedfortredere for rektor.
[6] I den eksterne testen kartla revisjonen hvilke ressurser kommunen har tilgjengeliggjort mot internett, hvorpå åpne porter, tilgjengelige tjenester og protokoller ble identifisert. Videre ble det gjennomført analyser av eventuelle feilkonfigurasjoner og manglende sikkerhetsoppdateringer blant de identifiserte tjenestene.
[7] Én av disse var konfigurert som en regulær PC for ansatte, én som en elev-PC, og én var uten restriksjoner. Ved å benytte tildelte testbrukere simulerte testen situasjoner hvor bruker med tilsvarende rettigheter er kompromittert eller forsøkes utnyttes av eksisterende bruker.

I tillegg til den tekniske testen av kommunens IKT-systemer, har revisjonen gjennomført en sikkerhetstest av fagsystemet *itslearning*.[8] Formålet med denne var å vurdere hvorvidt fagsystemets sikkerhets-mekanismer for å hindre uautorisert tilgang til brukerdata og administrativ funksjonalitet. Fagsystemet er nettbasert, og testen ble gjennomført fra revisjonens lokaler. Testen ble gjennomført fra perspektivet til de tre brukergruppene «elev», «lærer» og «administrator», og det ble gjort ulike kontrollerte forsøk på å bryte sikkerhetsmekanismene mellom brukergruppene og internt i brukergruppene.

All sikkerhetstesting er forbundet med en viss risiko. Etter nærmere avtale med kommunen ble det derfor avtalt en rekke risikoreduserende tiltak for gjennomføringen av sikkerhetstestene. Blant annet ble testene gjennomført innenfor spesifikt avtalte tidsvinduer, og det ble ikke gjennomført tjenestenektangrep[9] eller tilsvarende destruktive tester.

De tekniske rapportene etter sikkerhetstestene er å finne i vedlegg 6 og vedlegg 7. Vedleggene er unntatt offentlighet etter offentlighetsloven § 24 tredje ledd.

1.4.5 Nettfiskeforsøk

For å teste i hvilken grad de ansatte i skolen har kjennskap til retningslinjer og rutiner for informasjonssikkerhet, ble det gjennomført et kontrollert nettfiskeforsøk.[10] Revisjonen sendte en offisielt-utseende men falske e-post for å undersøke om og i hvilken grad ansatte i skolen i Bergen kommune følger retningslinjer knyttet til trygg bruk av e-post.

Bergen kommune har tekniske sikkerhetsmekanismer som måtte slås av for at nettfiskeforsøket skulle kunne gjennomføres. Kommunen har også rutiner knyttet til hendelseshåndtering som ble stanset for å tillate gjennomføringen av forsøket.

Rapporten fra nettfiskeforsøket er å finne i vedlegg 5.

1.4.6 Verifiseringsprosesser

Oppsummering av intervju er sendt til de som er intervjuet for verifisering og det er informasjon fra de verifiserte intervjureferatene som er benyttet i rapporten.

Datadelen av rapporten er sendt til byråden for verifisering, og faktafeil ble rettet opp i den endelige versjonen. Høringsutkast av rapporten ble sendt til byråd for barnehage, skole og idrett for uttale. Også i etter høringen ble det gjort justeringer i rapporten. Høringsuttalen er å finne i vedlegg 1, og revisjonens kommentar til denne er å finne i vedlegg 2.

1.5 Revisjonskriterier

Revisjonskriterier er de krav og forventninger som forvaltningsrevisjonsobjektet skal bli vurdert opp mot. Kriteriene er utledet fra autoritative kilder i samsvar med kravene i gjeldende standard for forvaltnings-revisjon. I dette prosjektet er revisjonskriteriene i hovedsak hentet fra *Lov om behandling av person-opplysninger* (personopplysningsloven). Kriteriene er nærmere presentert innledningsvis i hvert kapittel, og i sin fullstendighet i vedlegg 3.

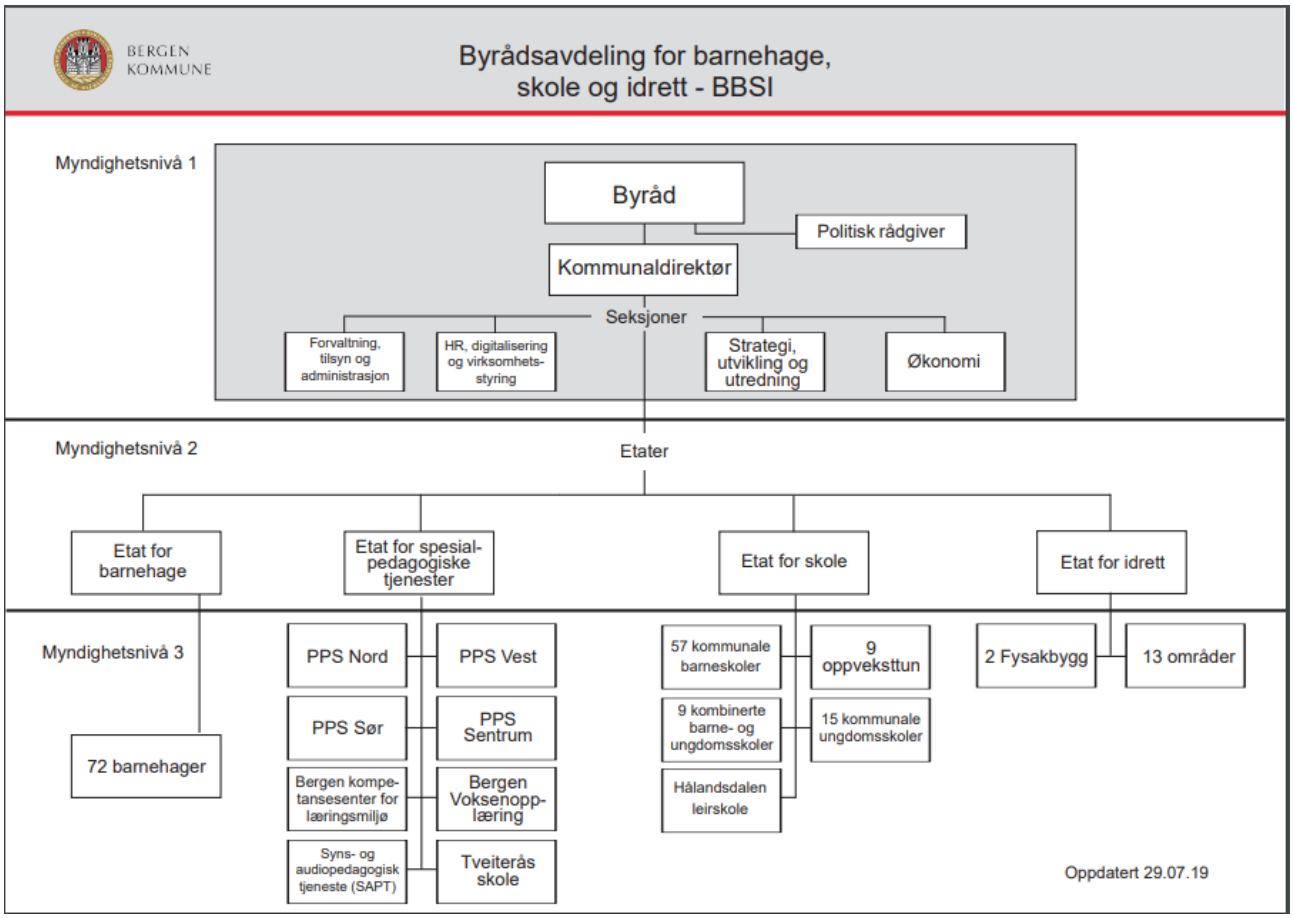
[8] *itslearning* ble valgt som fagsystem for sikkerhetstesten tidlig i revisjonsperioden. Som nevnt var forvaltningsrevisjonen i all hovedsak gjennomført før informasjonssikkerhetsbruddet knyttet til Vigilo inntraff.
[9] Se: https://no.wikipedia.org/wiki/Tjenestenektangrep
[10] Nettfisking benevnes også som «phising» eller «phisking».

2. Om tjenesteområdet

2.1 Organisering

Byrådsavdelingen for barnehage, skole og idrett (BBSI) er fra 1. juli 2019 organisert i en etatsmodell som vist i figur 1.[11]

Figur 1: Organisering av BBSI fra 1. juli 2019[12]



Byrådsavdelingen er slik organisert med tre myndighetsnivåer. Myndighetsnivå 1 omfatter seksjonene og kommunaldirektørene, mens etatene hører inn under myndighetsnivå 2. Resultatenhetene er myndighets-nivå 3 og innbefatter blant annet skolene i kommunen. Det fremgår av Bergen kommunes intranettsider, *Allmenningen,* at etatsmodellen som legges til grunn for BBSI er områdebasert og samsvarer med områdeinndelingen i de øvrige byrådsavdelingene. En etatsdirektør leder hver av de nyetablerte etatene.[13]

Kommunen opplyser at ansvaret for informasjons- og systemsikkerhet etter omorganiseringen ligger til seksjon for HR, digitalisering og virksomhetsstyring som er plassert under kommunaldirektøren på myndighetsnivå 1. Etter planen skal etatslederen gjennom områdelederne legge til rette for at skolene etterlever informasjonssikkerheten, mens systemeiere og systemkoordinatorer beholder ansvaret for at systemene tilfredsstiller krav til konfidensialitet, tilgjengelighet og integritet.

[11] Vedtatt i Byrådet 08.11.2018 i sak nr. 1262/18. Før omorganiseringen var skoleområdet organisert som en seksjon under fagavdeling for barnehage og skole. Systemansvarlige og systemkoordinatorer hørte gjennom denne organiseringen til fagavdelingen for barnehage og skole. I tillegg var områdelederne organisert i direkte linje under kommunaldirektøren og direkte overordnet resultatenhetene.
[12] Kilde: bergen.kommune.no
[13] https://allmenningen.bergen.kommune.no/aktuelt/nye-bbsi/etablerer-etatsmodell-i-byradsavdelingen

3. Rutiner og ansvar for informasjonssikkerhet

3.1 Problemstilling

I dette kapittelet vil vi svare på følgende hovedproblemstilling:

Har skolesektoren etablert klare rutiner og ansvarsforhold med hensyn til informasjonssikkerhet i samsvar med kommunens styringssystem for informasjonssikkerhet?

3.2 Revisjonskriterier

Artikkel 24 og 28 i forordningen omhandler den behandlingsansvarlige og databehandleren sitt ansvar for å etablere internkontroll; nr. 1 i artikkel 24 sier blant annet at den behandlingsansvarlige skal «gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov», mens artikkel 28 nr. 1 stiller krav om at databehandlere skal gi tilstrekkelig med garantier «for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordningen og vern av den registrertes rettigheter.»

Personvernforordningen artikkel 32 nr. 1 stiller videre krav om informasjonssikkerhet ved behandling av personopplysninger. Kravene som stilles er at informasjonssikkerheten skal være tilfredsstillende med hensyn til personopplysningene sin konfidensialitet, integritet, tilgjengelighet og robusthet gjennom at det blir satt i verk egnede tekniske og organisatoriske tiltak basert på risikovurderinger. Artikkelen inneholder regler som omhandler hva risikovurderingene skal legge vekt på.

I tillegg til reglene i personvernforordningen knyttet til internkontroll og informasjonssikkerhet, er kommunen gjennom eForvaltningsforskriften § 15 forpliktet å ha et internkontrollsystem basert på anerkjente standarder for styringssystem for informasjonssikkerhet:

> Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.
>
> Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.

Direktorat for forvaltning og IKT (Difi) er pekt ut som ansvarlig for å gi anbefaling knyttet til hvilket styringssystem for informasjonssikkerhet som bør benyttes. Difi anbefaler at offentlige virksomheter baserer seg på ISO/IEC 27001:2013, som er en internasjonal standard for styringssystem for informasjonssikkerhet.

Se vedlegg 3 for utfyllende revisjonskriterier.

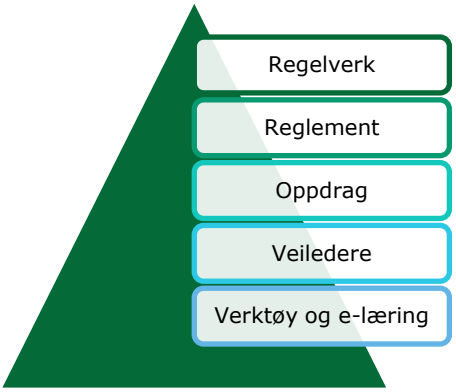
3.3 Datagrunnlag

3.3.1 Styrende dokumenter for informasjonssikkerhet i kommunen

Bergen kommune har gjennom ulike styrende dokumenter etablert et styringssystem for informasjons-sikkerhet. Særlig sentralt i dette er *Reglement for trygg digitalisering* og *Veileder for trygg digitalisering*. I tillegg inngår en rekke prosedyrer, retningslinjer, rutiner og oppdragsbeskrivelser i styringssystemet.

Den hierarkiske oppbyggingen av styringssystemet i Bergen kommune er som vist i figur 2:

Figur 2: Hierarkisk oppbygging av styringssystemet for informasjonssikkerhet og personvern[14]



Reglement for trygg digitalisering er det overordnete styringsdokumentet for informasjonssikkerhet i Bergen kommune. Reglementet gjelder alle arbeidstakere i Bergen kommune, og omfatter all behandling av informasjon i kommunen (både elektronisk og manuell), samt alle systemer som brukes til behandling av informasjon.

Reglementet fastslår innledningsvis sentrale delegeringer og definisjoner. Det går blant annet frem at ansvaret for behandling av personopplysninger ligger hos hver enkelt virksomhetsleder i kommunen, altså øverste ledere av enten en byrådsavdeling med underliggende resultatenheter, bystyrets administrasjon, eller kommunalt foretak.[15]

Formålet med reglementet er videre definert som:

> å sikre god styring og kontroll med personvern og informasjonssikkerhet, å fastsette felles minimumskrav til den enkelte byrådsavdelings systematiske arbeid med personvern og informasjonssikkerhet, og å fremme god sikkerhetskultur.

Reglementet definerer fire overordnete sikkerhetsmål for kommunen, gjengitt i tabell 2:

Tabell 2: Sikkerhetsmål for personvern og informasjonssikkerhet

Nr.	Dimensjon	Mål
1.	Personvern	Vi ivaretar personvernet til ansatte og innbyggere.
2.	Konfidensialitet	Vi får bare se informasjon vi har rett til å se.
3.	Integritet	Vi kan stole på at informasjon vi behandler er korrekt.
4.	Tilgjengelighet	Vi får tilgang til rett informasjon, når vi trenger den.

Reglementet inneholder også rolle- og ansvarsbeskrivelser knyttet til informasjonssikkerhet (se tabell 4 på side 19).

3.3.2 Retningslinjer og rutiner i skolesektoren

I *Plan for smart oppvekst i Bergen - plan for digitalisering og innovasjon i barnehage, skole og idrett 2019 - 2022*[16] er ett av tiltakene i perioden å sikre trygg informasjonsbehandling. Det er under punktet om trygg informasjonsbehandling uthevet fem tiltak:

- Forbedre rutiner for informasjonssikkerhet og personvern

[14] Kilde: Veileder for trygg digitalisering.
[15] Med andre ord er de behandlingsansvarlige i Bergen kommune kommunaldirektører, bystyredirektør eller direktører for kommunale foretak.
[16] Plan for smart oppvekst i Bergen. Plan for digitalisering og innovasjon i barnehage, skole og idrett 2019 – 2022. Vedtatt av Bergen bystyre 30.01.2019 i sak 9/19

- Innføring av nytt saks- og arkivsystem (BK360)
- Innføre to-faktor pålogging eller andre sikringstiltak for å følge anbefalingene fra Datatilsynet
- Identifisere og realisere digitaliserings- og innovasjonselementer fra *Forenklingsutvalget*[17]
- Etablere en strategisk og operativ IKT-gruppe for informasjonssikkerhet

Til det første punktet om rutiner fremgår det at byrådsavdelingen vil foreta en kvalitetssikring av alle digitale systemer og rutiner, gjennomføre opplæring knyttet til personopplysninger i digitale system og tydeliggjøre rolleforståelse blant data-, system- og prosesseiere. Det står videre at det vil bli etablert rutiner for at innkjøp av for eksempel programmer og applikasjoner blir gjort i henhold til sentrale retningslinjer og at programvare er godkjent av *sentral systemansvarlig*.[18]

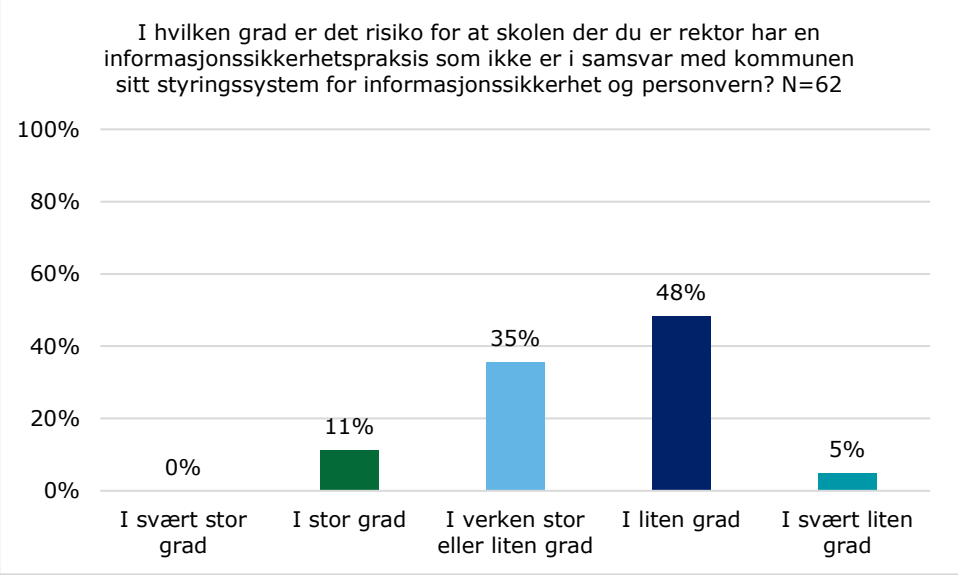
Det blir i planen vist til at man i byrådsavdelingen skal videreutvikle bruken av, og legge til rette for tilgang til skytjenester. Under dette fremgår det at alle programmer som skal tas i bruk på PC-er, Chromebooks eller nettbrett i enhetene, skal godkjennes av byrådsavdelingen. Dette for å sikre god kvalitet på tjenestene, ivareta informasjonssikkerheten, samt sikre likhet på tvers av enhetene.

Revisjonen får opplyst at det høsten 2018 ble arbeidet med informasjonssikkerhet i BBSI samlet under programmet for *Smart oppvekst i Bergen*. Kommunen opplyser videre at arbeidet med informasjons-sikkerhet knyttet til informasjonssystemene i BBSI frem til 2018 har vært ivaretatt av pedagogisk IKT-koordinator sammen med rådgivere i seksjon skole under den gamle fagavdeling barnehage og skole.

Det fremgår i intervju at det ikke er utarbeidet egne overordnede rutiner knyttet til informasjonssikkerhet i skolene fra BBSI sin side utenom systemsikkerhetsrutiner tilhørende de enkelte IKT-systemene som blir benyttet i skolene.

I spørreundersøkelsen blant rektorene ble de stilt spørsmål om i hvilken grad det er risiko for at skolen har en informasjonssikkerhetspraksis som ikke samsvarer med kommunen sitt *Styringssystem for informasjonssikkerhet og personvern*. Svarene er gjengitt i figur 3:

Figur 3: Risiko for avvikende informasjonssikkerhetspraksis

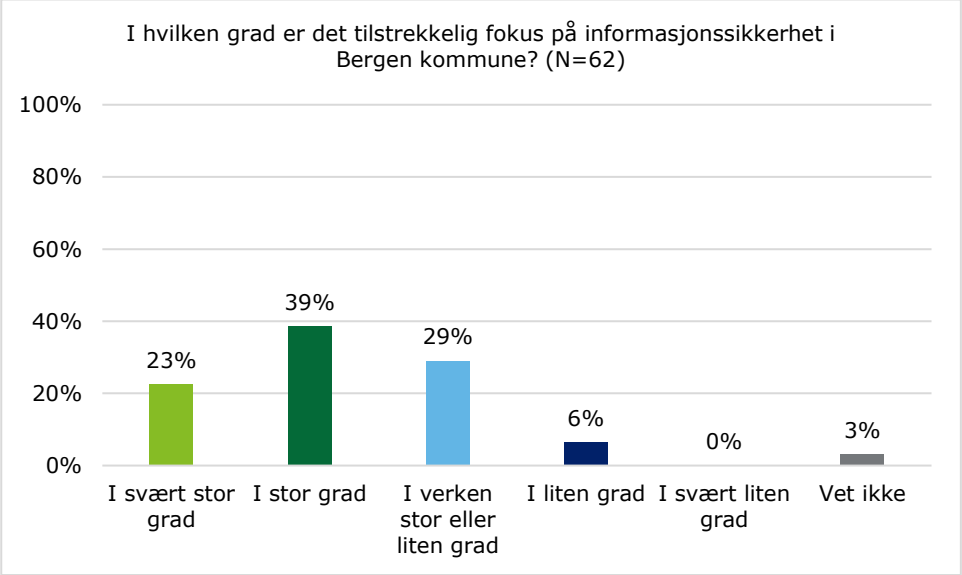


Som vist i figuren over svarer 35 % av respondentene at det «i verken stor eller liten grad» er risiko for at skolene sin informasjonssikkerhetspraksis ikke samsvarer med styringssystemet for informasjonssikkerhet og personvern. 11 % av rektorene svarer at det «i stor grad» er risiko for dette.

[17] Rapport fra Forenklingsutvalget for barnehage og skole 2015: https://www.bergen.kommune.no/politikere-utvalg/api/fil/331550/Rapport-Forenklingsutvalget
[18] Det fremgår ikke hvilken rolle som har ansvar som sentral systemansvarlig.

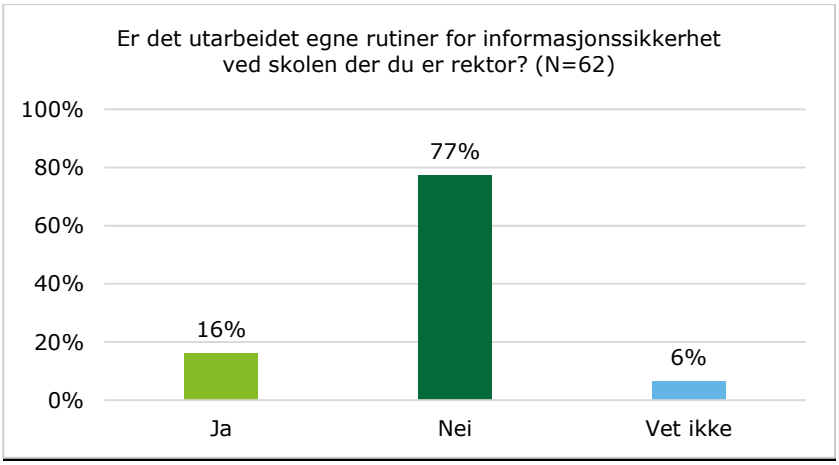
Rektorene som deltok i spørreundersøkelsen fikk videre spørsmål om i hvilken grad de opplever at det er tilstrekkelig fokus på informasjonssikkerhet i kommunen. Svarene er gjengitt i figur 4, og som det fremgår der, svarer langt de fleste enten «i svært stor grad» (23 %) eller «i stor grad» (39 %) på spørsmålet:

Figur 4: Fokus på informasjonssikkerhet



Rektorene fikk også spørsmål om det er utarbeidet egne rutiner for informasjonssikkerhet ved skolen der vedkommende er rektor. På dette spørsmålet svarer 77 % av respondentene «nei» og 6 % svarer «vet ikke» (figur 5):

Figur 5: Informasjonssikkerhetsrutiner ved skolene



Respondentene som svarte «ja» på spørsmålet ble bedt om å gi en beskrivelse av hvilke informasjonssikkerhetsrutiner som er utarbeidet ved skolen.[19] Flere av dem som svarte viser til at skolen har rutiner på å ikke sende sensitiv informasjon via e-post.[20]

[19] N=7.

[20] Tre av respondentene viser til at skolen benytter BK360 for korrespondanse knyttet til sensitive opplysninger, mens to svarer at de er i gang med å ta i bruk BK360. To av respondentene viser til at elevmapper legges i BK360 og en annen respondent svarer at disse mappene er låst inne i brannsikre skap og at bare rektor og konsulent har nøkler til skapene. Videre nevnes det blant annet enkeltvis: kurs i GDPR for ansatte, skriftlig godkjenning fra foreldre ved utsending av informasjon til tannlege eller andre, rutiner for bruk av IKT ved skolen formidlet til elever og foresatte, ingen lagring av sensitive opplysninger på minnepenn eller egne områder på PC.

Rektorene som oppgir at det er utarbeidet egne informasjonssikkerhetsrutiner på skolene fikk også et oppfølgingsspørsmål om hvorvidt det er risiko for at disse rutinene ikke samsvarer med kommunen sitt styringssystem for informasjonssikkerhet og personvern.[21] På dette spørsmålet svarer seks av ti respondenter at det er i liten eller svært liten grad er risiko for dette, mens fire mener at det «i verken stor eller liten grad» er risiko for dette.

3.3.3 Overordnet ansvar for informasjonssikkerhet

Bergen kommune gjør rede for sentrale og overordnete ansvarsoppgaver, roller, oppgaver og fullmakter gjennom styrende dokumenter i styringssystemet for personvern og informasjonssikkerhet

Reglement for trygg digitalisering inneholder beskrivelse og oversikt over rolle- og ansvarsbeskrivelser knyttet til informasjonssikkerhet beskrevet i tabellform. Roller innenfor skolesektoren med ansvar for informasjonssikkerhet er gjengitt i tabell 3 under[22]:

Tabell 3: Ansvar for informasjonssikkerhet i Bergen kommune

Organisasjonsnivå	Rolle	Beskrivelse
Byrådsavdeling med linjeansvar (byrådsavdelingene nivå 1) og bystyrets adm. organer	**Kommunaldirektør**	Se til at lover, regler og politiske vedtak følges samt at konsernsystemer benyttes. Utarbeide/forvalte sektorspesifikke systemer, rutiner og verktøy, og se til at disse brukes/følges. Ivareta rollen som behandlingsansvarlig. Utarbeide, operasjonalisere og rapportere på sikkerhetsmål Sørge for at ledelsens gjennomgang gjennomføres. Gi veiledning overfor underliggende enheter. Gjennomføre etterkontroller på utvalgte områder i egen byrådsavdeling.
Resultatenhet	**Resultatenhetsleder**	Se til at lover, regler, politiske vedtak følges samt at konsern-, etats- og fagspesifikke systemer benyttes. Utarbeide/forvalte fagspesifikke systemer, rutiner og verktøy der dette ikke ivaretas på overordnet nivå. Ivareta rollen som behandlingsansvarliges representant Etablere nødvendig egenkontroll som sikrer riktig praksis. Sørge for nødvendig kompetanse i egen enhet.

I *Veileder for trygg digitalisering*, som er et supplement til *Reglement for trygg digitalisering*, fremgår det at ansvaret som behandlingsansvarlig er delegert fra Byrådet til kommunaldirektørene i de ulike byrådsavdelingene. Det står videre at oppfølgingen av behandlingsansvaret gjøres gjennom informasjonssikkerhetsforum (se tabell 4 nedenfor).

3.3.4 Oppgaver og roller knyttet til informasjonssikkerhet

Beskrivelse av overordnede roller og oppdrag i forbindelse med informasjonssikkerhet i kommunen fremgår av *Reglement for trygg digitalisering*. For kommunaldirektør, leder av EDD, systemeiere og resultatenhetsledere foreligger det videre egne oppdragsbeskrivelser og mandater for informasjonssikkerhet. I tillegg er det utarbeidet mandat for personvernombud og informasjonssikkerhetsforum, samt *Krav til akseptabel bruk av IKT* for alle ansatte i kommunen. Rolle- og oppdragsbeskrivelsene som fremstilt i *Reglement for trygg digitalisering* er gjengitt i tabell 4:

[21] N=10

[22] Tabellen i *Reglement for trygg digitalisering* viser også til BFIEs ansvar for informasjonssikkerhet som byrådsavdeling med konsernansvar. Det skilles mellom *policynivå* (kommunaldirektør for HR, digitalisering og eiendom og direktør for seksjon for digitalisering og innovasjon) og *driftsnivå* (kommunaldirektør for HR, digitalisering og eiendom, direktør for seksjon for digitalisering og innovasjon og leder for enhet for digitale driftstjenester).

Tabell 4: Informasjonssikkerhetsroller

Rolle	Beskrivelse	Oppdragsbeskrivelse
Kommunaldirektør	Kommunens øverste administrative ledelse er å anse som det regelverket kaller «behandlingsansvarlig» i den enkelte byrådsavdeling.	Behandlingsansvarlig skal sørge for at personvernregelverket etterleves i egen virksomhet og følge opp at ledere, systemeiere og ansatte følger sine respektive oppdragsbeskrivelser. I praksis foregår dette gjennom deltakelse i informasjons-sikkerhetsforum og ledelsens gjennomgang med kommunens personvernombud.
Personvernombud	Pålagt rolle i personvernregelverket. Personvernombudet skal rapportere direkte til øverste ledelse. Ombudet skal også samarbeide med og være kontaktpunkt for tilsynsmyndigheten.	Personvernombudet har etter regelverket definerte oppgaver og skal bistå kommunens ledelse med å være i samsvar med personvernregelverket, herunder også krav til informasjonssikkerhet.
Informasjons-sikkerhetsforum	Et forum for samordning av arbeidet med ivaretakelsen av personvern og informasjonssikkerhet. Forumet består av én representant fra hver byrådsavdeling og bystyrets organer, personvernombudet og sikkerhetsfaglig kompetanse.	Informasjonssikkerhetsforum følger i praksis opp kommunens styring av personvern og informasjonssikkerhet, vurderer risiko opp mot eksisterende tiltak og foreslår planer for endringer og forbedringer av «Reglement for trygg digitalisering» og konkrete sikringstiltak.
Leder av Enhet for digitale driftstjenester	Er ansvarlig for den tekniske ivaretakelsen av IKT-sikkerheten i kommunens IKT-infrastruktur.	Skal sørge for at kommunens digitale driftsenhet følger opp og iverksetter nødvendige tekniske sikringstiltak.
Resultatenhetsleder	Alle resultatenhetsledere i kommunens ulike resultatenheter har rollen regelverket kaller «behandlingsansvarliges representant».	Skal sørge for at kommunens styrende dokumenter for personvern og informasjonssikkerhet følges opp i egen resultatenhet.
Systemeier	Alle som har formelt ansvar for et IKT-system/-tjeneste i kommunen. Et hvert IKT-system krever ulike tiltak for å ivareta godt personvern og god informasjonssikkerhet.	Skal sørge for at Reglement for trygg digitalisering blir fulgt i forbindelse med anskaffelse, implementering og forvaltning av systemet som vedkommende har ansvaret for.
Ansatt	Alle ansatte forvalter ulike former for informasjon og har derfor en viktig rolle i arbeidet med å ivareta personvern og informasjonssikkerhet i kommunens virksomhet.	Skal sørge for å ivareta personvern og informasjonssikkerhet i eget arbeid og følge de regler og veiledere som gjelder innenfor eget ansvarsområde.

I mandat- og oppdragsbeskrivelsene utdypes ansvaret til rollene nevnt i tabellen over knyttet til blant annet oversikt, avvik, beredskap og opplæring for å ivareta krav til personvern og informasjonssikkerhet. Det er ikke lagt inn beskrivelse av rolle og/eller oppdrag tilknyttet informasjonssikkerhet for andre roller, som systemkoordinator eller IKT-koordinator, i *Reglement for trygg digitalisering*. Dette er roller som i skole-sektoren i praksis har ansvar og oppgaver knyttet til informasjonssikkerhet (se avsnitt 3.3.5 og 3.3.6).

I intervju blir det fortalt at det ikke er klare roller og ansvar knyttet til informasjonssikkerhet i byråds-avdelingen. Det er ikke klart hvem som eier de overordnete og koordinerende oppgavene på feltet, samtidig som det på revisjonstidspunktet ikke var noe reelt mellomledd mellom kommunaldirektøren og rektorene når det gjelder informasjonssikkerhet.[23]

[23] Kommunen viser i forbindelse med verifiseringen av rapporten til fagfullmaktene av 2. februar 2017, punkt 1 om områdelederne og fagdirektør for barnehage og skole sine delegerte fullmakter, som sier at disse skal «se til at skoler, barnehage og PPS gir tjeneste i henhold til gjeldende lov- og regelverk, vedtatte økonomiske rammer og øvrige kommunale styringsdokument og føringer». Informasjonssikkerhet er ikke særskilt nevnt i fagfullmaktene.

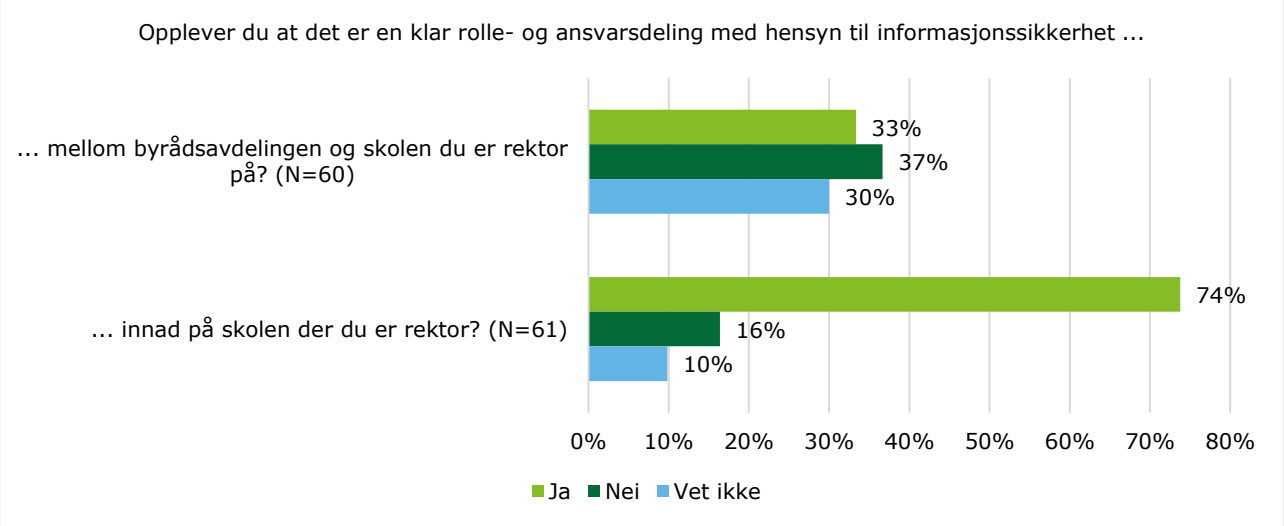
Som nevnt i seksjon 2.1, har den nyetablerte etatslederrollen et lederansvar for rektorene. Det går ikke frem av informasjon revisjonen har mottatt hvilket informasjonssikkerhetsansvar som ligger til denne rollen, men revisjonen får opplyst fra kommunen at det etter planen er områdelederne som skal legge til rette for at skolene ivaretar informasjonssikkerheten.[24]

Det går videre frem i intervju at det flere ganger og over tid har blitt meldt behov for en egen stilling eller deler av stilling tilknyttet informasjonssikkerhet på byrådsavdelingen.[25] I intervju pekes det på at IKT- og informasjonssikkerhet først ble et prioritert tema i byrådsavdelingen etter at det har blitt en økt oppmerksomhet på området, blant annet gjennom innføringen av ny personopplysningslov.

Det fremgår videre i intervju at det som ledd i omorganiseringen på BBSI er opprettet en stilling som rådgiver for informasjonssikkerhet.[26] Denne stillingen har ansvar for informasjonssikkerhet hos BBSI gjennom å blant annet følge opp at alle system er i henhold til krav og at resultatenhetene følger regelverk og gjennomfører tilstrekkelig opplæring. Tanken er at stillingen skal operere i grensesnittet mellom Seksjon for digitalisering og innovasjon konsern (SDI) og Enhet for digitale driftstjenester (EDD) hos byrådsavdelingen. Kommunen understreker i forbindelse med verifiseringen av rapporten at det i forbindelse med omorganiseringen av BBSI er opprettet en seksjon for HR, digitalisering og virksomhets-styring på byrådsavdelingen som blant annet skal bedre ivareta informasjonssikkerhetsområdet i tett samarbeid med andre sentrale IKT-faglige miljø i kommunen.

I spørreundersøkelsen til rektorene, ble det stilt spørsmål om hvorvidt de opplever at det er en klar rolle- og ansvarsdeling med tanke på informasjonssikkerhet 1) mellom byrådsavdelingen og skolen og 2) innad på skolen:

Figur 6: Rolle- og ansvarsdeling



Figur 6 viser at 37 % av respondentene opplever at det ikke er en klar ansvarsdeling mellom byråds-avdelingen og skolen med hensyn til informasjonssikkerhet, mens 30 % svarer «vet ikke» på spørsmålet.

[24] Kommunen understreker i forbindelse med verifiseringen av rapporten at etatsdirektøren får sine fullmakter fra kommunaldirektøren og kan videredelegere disse. Det er ikke slik at områdelederne får ansvar fra kommunaldirektøren.
[25] Det blir opplyst at dette behovet har blitt meldt over tid i medarbeidersamtaler og i møter, men at en egen stilling innen informasjonssikkerhet først ble tydelig brakt på banen i forbindelse med ny GDPR lovgiving våren 2018.
[26] Revisjonen får per 9.8.2019 opplyst at det ikke er ansatt noen i denne stillingen ennå, men at det er igangsatt en prosess på dette. Det er en innleid ressurs med relevant kompetanse som har ansvar som rådgiver innen informasjonssikkerhet i påvente av endelig ansettelse.

3.3.5 Systemeier og systemkoordinator

Reglement for trygg digitalisering beskriver i korte trekk systemeiers rolle og oppgaver når det gjelder informasjonssikkerhet og personvern (se tabell 4). Reglementet viser videre til *Oppdrag – personvern og informasjonssikkerhet for systemeiere* og har lenke til oppdragsbeskrivelsen på *Allmenningen*.

I oppdragsbeskrivelsen for systemeiere fremgår det hvilke oppgaver systemeier er ansvarlig for at blir etterlevd knyttet til oversikt, risiko, avvik og beredskap. Systemeiere er blant annet ansvarlige for at system meldes til kommunens personvernombud og at system er sikret i henhold til *Sjekkliste for grunnsikring av IKT-systemer i Bergen kommune.* Det er ikke lagt inn henvisning eller lenke til hvor denne sjekklisten er tilgjengelig.

Andre oppgaver innenfor systemeiers ansvarsområde er blant annet å sørge for en dokumentert rutine for håndtering og oppfølging av avvik knyttet til systemet og at det er gjennomført personvernkonsekvens-vurdering og teknisk risikovurdering.

Bergen kommunes *Styrende dokument for IKT og digitalisering* omtaler blant annet systemeierrollen i tillegg til rollen som systemkoordinator. Dette dokumentet er tilgjengelig på intranettet til kommunen, men ikke under menypunktene *Informasjonstjenester og IKT* eller *Informasjonssikkerhet og personvern.*

Tabell 5: Ansvar knyttet til systemeier- og systemkoordinatorrollen

Rolle	Ansvar
System-/tjenesteeier	System-/tjenesteeier er ansvarlig for å sikre et strategisk og langsiktig fokus for det aktuelle systemet og sikre best mulig utnyttelse for de arbeidsprosesser systemet understøtter. Systemeier er ansvarlig for at systemet tilfredsstiller gjeldende krav til blant annet informasjonssikkerhet og drifts- og vedlikeholdsavtaler. Systemeier skal: • i samarbeid med systemkoordinator ivareta at systemutvikling, -leveranser og -forvaltning utføres i henhold til brukernes og enhetenes behov, samt i henhold til etablerte avtaler, rammeverk og styrende dokumenter. • være ansvarlig for at planer og tiltak for nye og forbedrede systemer blir kravstilt og forankret iht. gjeldende IKT-strategi i Bergen kommune, samt ivareta realisering av gevinster for systemer som tas i bruk. • i samarbeid med Systemkoordinator og/eller SDI supplere denne rollebeskrivelsen ved behov for tilpasning til lokale forhold.
System-/tjeneste-koordinator	Systemkoordinator skal i samarbeid med systemeier koordinere, videreutvikle og forbedre systemet i henhold til brukernes behov. Systemkoordinator rapporterer til systemeier og vil blant annet ha ansvar for: • rutiner/opplegg for brukerstøtte • utarbeidelse av brukerdokumentasjon og rutiner • oppdatere konfigurasjonsdokument knyttet til oppgraderinger og eventuelle tilpasninger • rutiner/opplegg for brukerstøtte, feilmelding og bestillinger • ivareta informasjonssikkerhet, riktig funksjonalitet og leveransekvalitet for systemet • operativ forvaltning av systemet på vegne av systemeier (inkludert dialog med leverandør(er)), og skal arbeide i tett samarbeid med tjenestekoordinator(er) for eventuelt tilhørende tjenester • Ansvarlig for gjennomføring og koordinering av testing ved oppgraderinger på klientplattformen i Bergen kommune. • i samarbeid med systemeier og/eller SDI supplere denne rollebeskrivelsen ved behov.

Revisjonen har fått tilgang til en oversikt over administrative programmer og programmer på elevnett med blant annet tilhørende systemeier, systemkoordinator og hvem som kan gjøre bestillinger.[27] Programmene er klassifisert basert på om hvem som har tilgang (for eksempel om det finnes på alle PC-er, om alle har tilgang, om kun noen har tilgang, om tilgang er behovsprøvd, osv.)

Det er BBSI som har ansvar for systemene som brukes av enhetene i byrådsavdelingen, mens SDI har ansvar for fellessystem som benyttes av hele kommunen (for eksempel BK360). Dette fremgår også av

[27] http://iktweb02a.adm.bgo/SystemoversiktWeb/

oversikten over programmer, da alle program som utfra klassifiseringen finnes på alle PC-er, har systemeiere fra SDI og EDD. Når det gjelder program som brukes i skolesektoren, er flere av dem oppført med tidligere fagdirektør for skole og barnehage som systemeier.[28] I tillegg er det noen av programmene som ikke har tildelt systemeier.[29]

Det fremgår i intervju at informasjonssikkerhetsansvaret som påhviler systemeierrollen ikke har vært praktisert i henhold til kommunens styringssystem for informasjonssikkerhet og personvern. I dag er det seksjonssjef for HR, digitalisering og virksomhetsstyring som har rollen som systemeier på vegne av kommunaldirektøren.

Systemkoordinatorene forteller i intervju at de har fått delegert ansvar for informasjonssikkerhet tilknyttet informasjonssystemene fra systemeier. Det er formelt avklart hvem som er systemkoordinatorer for de ulike systemene, men det er ikke skriftliggjort at systemkoordinatorer har noe ansvar for informasjons-sikkerheten og heller ikke hva dette ansvaret innebærer.[30]

I intervju kommer det frem at verken systemkoordinatorene eller IKT-koordinator (se neste avsnitt) i særlig grad forholder seg til styringssystemet for personvern og informasjonssikkerhet eller andre overordnede rutiner eller retningslinjer knyttet til informasjonssikkerhet.[31] Revisjonen får fortalt at det i hovedsak er dokumentet *Retningslinjer for IT-sikkerhet i Bergen kommune*[32] fra 2002 disse forholder seg til når det gjelder beskrivelse av ansvar, roller og oppgaver innenfor IT-sikkerhet i kommunen. Tabell 6 under viser beskrivelsene av ansvar og oppgavene tilhørende henholdsvis IT-sikkerhetskoordinator, systemeier og systemkoordinator:

Tabell 6: Roller og ansvar beskrevet i Retningslinjer for IT-sikkerhet (2002)

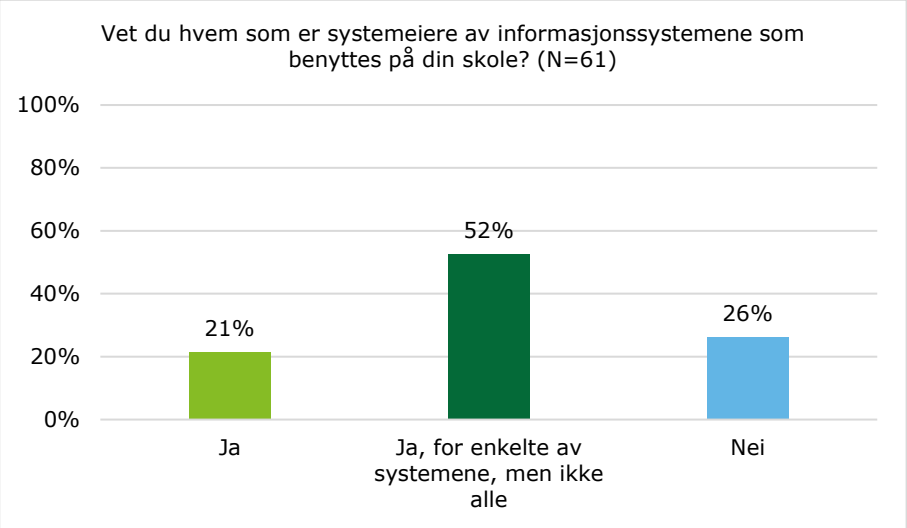
Rolle	Ansvar
IT-sikkerhetskoordinator	Har det daglige ansvaret for å koordinere og samordne alle forhold i arbeidet med informasjonssikkerheten i hele kommunen, og skal være kontrollinstans for å påse at de planer og rutiner IT-seksjonen og enhetene legger opp til, er gode nok og overholdes
Systemeier	Er den som er administrativt ansvarlig for den enheten/fagområdet som det enkelte system skal betjene. Behandlingsansvaret er som oftest delegert til systemeier. Systemeier er sikkerhetsmessig ansvarlig for sitt system
Systemkoordinator	Utpekes av systemeier og har det løpende ansvar for forvaltning og utvikling av systemet, herunder den daglige oppfølging og kontroll av sikkerhetsmessige oppgaver

Det går ikke frem ytterligere informasjon om rollene i dokumentet enn det som er vist i tabell 6.

Rektorene som deltok i spørreundersøkelsen fikk spørsmål om de kjenner til hvem som er systemeiere av informasjonssystemene som benyttes på deres skole. Som fremstilt i figur 7 under svarer 26 % «nei», mens 52 % kjenner til hvem som er systemeiere for enkelte av systemene, men ikke alle; 21 % svarer «ja».

[28] Tidligere fagdirektør gikk av med pensjon ved årsskiftet 2018/2019.
[29] På revisjonstidspunktet inngikk ikke Vigilo i kommunens sentrale systemoversikt. Kommunen opplyser i forbindelse med høringen av rapporten at dette sannsynligvis beror på en misforståelse, og peker videre på at den sentrale systemoversikten er en oversikt over systemer supportert via EDD og i hovedsak tilknyttet det administrative nettet i Bergen kommune. Vigilo er supportert via EDD men da i forbindelse med eFeide og brukerkontoer. Det gjenstår fra BBSI å bestille en tjeneste rundt Vigilo for å få det inn på den listen når prosjektet skal i drift. Men Vigilo er, i likhet med mange andre tjenester i bruk i skolene, kun registrert i totaloversikten for systemer i bruk i BK som Avdeling for informasjonssikkerhet og personvern registrerer og oppdaterer.
[30] I forbindelse med verifiseringen av rapporten viser kommunen til at det i lengre tid har vært formalisert hvem som er systemkoordinator og hvem som er systemeier for de ulike systemene, og at dette er skriftliggjort.
[31] Systemkoordinatorene legger til at dette vil variere noe mellom systemkoordinatorer og størrelsen på systemene de har ansvar for.
[32] Retningslinjer for IT-sikkerhet. Bergen kommune. Bergen, desember 2002.

Figur 7: Kjennskap til hvem som er systemeiere



3.3.6 IKT-koordinator

BBSI har to IKT-koordinatorer; én med ansvar for pedagogiske system (Pedagogisk IKT-koordinator) og én med ansvar for administrative system (IKT-koordinator). Kommunen opplyser at IKT-koordinator er en sentral ressurs når det gjelder informasjonssikkerhet og bestilling av programvare i BBSI. Det fremgår videre at IKT-koordinator etter omorganiseringen tilhører seksjon for HR, digitalisering og virksomhets-styring på BBSI.

I intervju fremgår det at IKT-koordinator ikke formelt har fått tildelt ansvar for informasjonssikkerhet, men på eget initiativ har tatt noe ansvar for dette. Han har for eksempel ved anledning påpekt overfor ledelsen at det er behov for mer oppmerksomhet rettet mot informasjonssikkerhet i skolene, og forteller at han er behjelpelig med å svare på e-poster fra ansatte på temaet. IKT-koordinator har i flere perioder vært i permisjon fra stillingen sin. I disse periodene har det ikke vært andre som har ivaretatt dette ansvaret.[33]

Pedagogisk IKT-koordinator forteller at det i hans rolle er det pedagogiske som har hovedfokus, blant annet gjennom å kommunisere ut nytten av digitale læringssystem og digitale verktøy til IKT-kontakter og lærere i skolene. Pedagogisk IKT-koordinator forteller videre at man vil finne hans navn i EDDs liste over systemeiere i kommunen, men at rollen som pedagogisk IKT-koordinator aldri har hatt et faktisk ansvar for informasjonssikkerheten i systemene. Han peker videre på at det er IKT-koordinator (for administrative system) som er IKT-ansvarlig og som har hatt ansvar for systemsikkerheten i skolenes IKT-systemer.

Som nevnt over fremgår det i intervju at IKT-koordinator, til liks med systemkoordinatorene, ikke i stor grad kjenner til kommunens *Styringssystem for informasjonssikkerhet og personvern***.** IKT-koordinator forholder seg til IKT-strategi for kommunen, tjenestekatalog og rutiner for melding av avvik, og søker ellers på tema innenfor området på *Allmenningen* ved behov.

3.3.7 Resultatenhetsleder

I *Reglement for trygg digitalisering* går resultatenhetsleders ansvar, rolle og oppgaver knyttet til informasjonssikkerhet og personvern frem (se tabell 3 og tabell 4 over). Under oppgavebeskrivelsen blir det vist til *Oppdrag – personvern og informasjonssikkerhet for resultatenhetsledere*[34] med lenke til dokumentet på *Allmenningen*.

I oppdragsbeskrivelsen fremgår det hvilke oppgaver resultatenhetsleders er ansvarlig for at blir etterlevd knyttet til oversikt, risiko, avvik, beredskap og opplæring. Blant annet er resultatenhetsleder ansvarlig for at enheten fører en dokumentert oversikt over hvilken informasjon den behandler, hvor og av hvem. Videre skal resultatenhetsleder påse at enheten har en dokumentert plan for å håndtere situasjoner som følge av

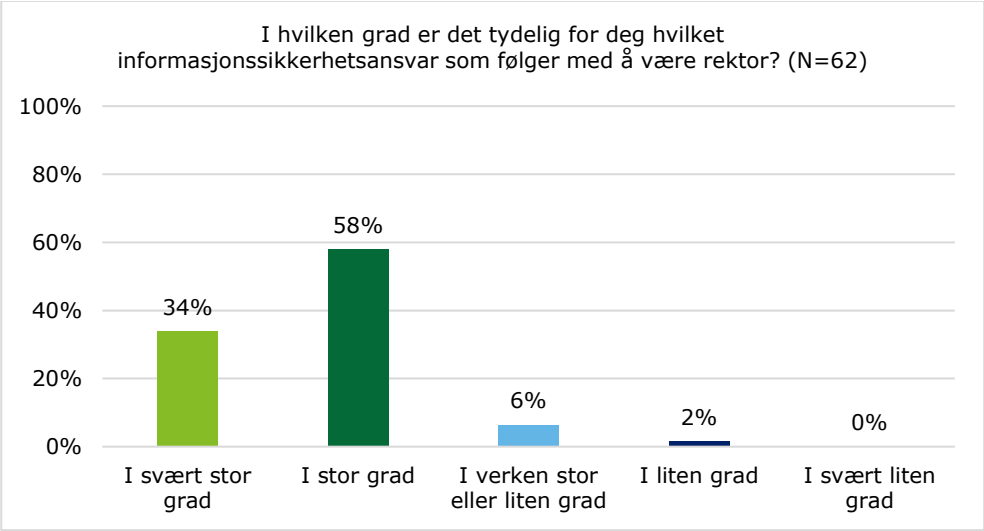
[33] I forbindelse med høringen av rapporten kommenterer kommunen at de nevnte permisjonene ble avviklet juni 2003 til august 2004, fra mai 2007 til august 2008, og fra september 2011 til januar 2013.
[34] Oppdrag – personvern og informasjonssikkerhet for resultatenhetsledere. Ikke datert.

at for eksempel personvernet til de ansatte eller innbyggerne ikke er ivaretatt. Det fremgår òg at oppfølging av informasjonssikkerhetsarbeidet ligger til hver enkelt rektor i skolene.

Ved utsending av spørreundersøkelse til rektorene i skolene i Bergen fikk de en e-post der revisjonen åpnet for at rektor kan svare på undersøkelsen sammen med én eller flere ansatte ved skolen dersom for eksempel ansvaret for informasjonssikkerhet er videredelegert. Én av 62 respondenter oppgir at ansvaret er videredelegert.[35]

I spørreundersøkelsen til rektorene i kommunens skoler fikk respondentene spørsmål om i hvilken grad informasjonssikkerhetsansvaret som følger med å være rektor er tydelig. Svarene fremgår i figur 8:

Figur 8: Tydelig informasjonssikkerhetsansvar som rektor

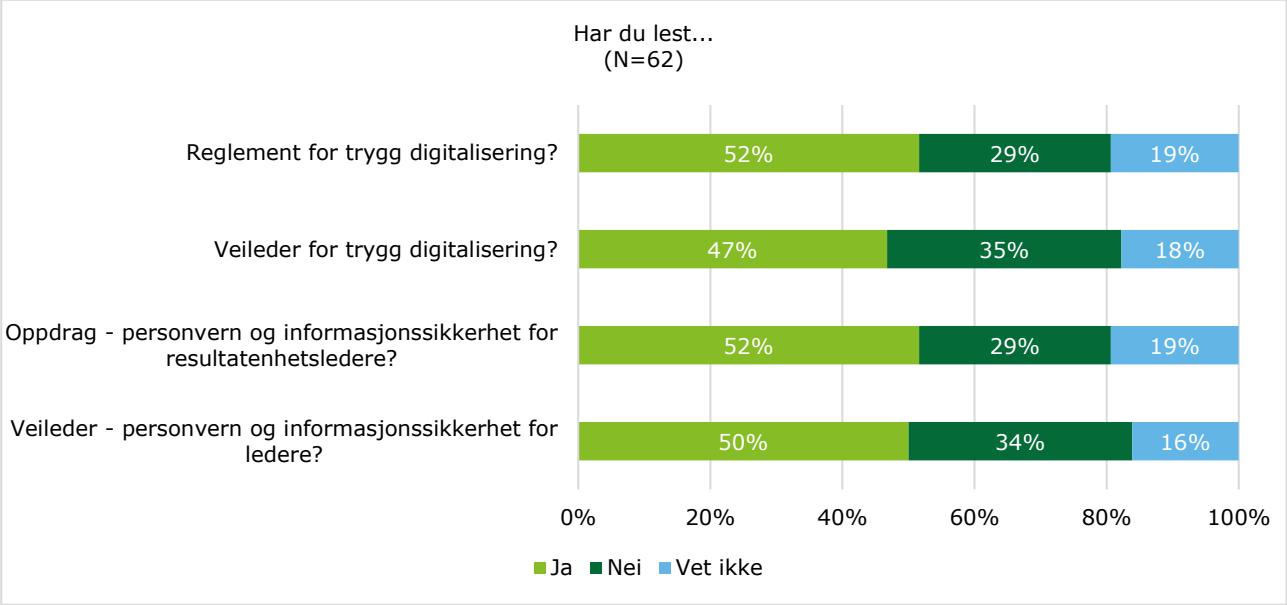


Som vist i figuren svarer til sammen 92 % at det «i svært stor grad» eller «i stor grad» er tydelig hvilket informasjonssikkerhetsansvar som følger med å være rektor.

Rektorene fikk videre spørsmål om de har lest sentrale styringsdokument tilhørende *Styringssystem for informasjonssikkerhet og personvern* i Bergen kommune. Svarene er gjengitt i figur 9:

[35] Det var fire rektorer som svarte på spørreundersøkelsen sammen med andre, men bare én som oppgir at dette er en ansatt med videredelegert ansvar for informasjonssikkerhet og personvernansvar.

Figur 9: Kjennskap til styringsdokument



Som vist i figur 9, svarer rundt halvparten «ja» på de fire delspørsmålene, mens mellom 29 % og 35 % svarer «nei», og mellom 16 % og 19 % svarer «vet ikke».

Oversikt over personopplysninger

Reglement for trygg digitalisering stiller krav til at den enkelte resultatenhet må ha oversikt over person-opplysningene som behandles:

- Den enkelte resultatenhet må sørge for at relevante deler av kommunens protokoll for behandling av personopplysninger til enhver tid er korrekt og at eventuelle endringer blir oppdatert og offentliggjort på kommunens nettsider.
- Enhver resultatenhet som setter i verk en ny eller endrer en behandling av personopplysninger, det være seg i form av nye IKT-systemer eller -tjenester, skjemaer eller annet, plikter ved lov å melde dette til kommunens personvernombud, som skal bistå resultatenheten med å vurdere lovlighet og tilstrekkelig sikring.

Reglementet viser videre til kommunens intranettside *Melding om behandling av personopplysninger*.[36] Her får man oversikt over hva som skal meldes, en forklaring på hva som er personopplysninger og sensitive personopplysninger, hvilken lovgivning som gjelder taushetsbelagte opplysninger, samt kontakt-informasjon til kommunens personvernombud. Det er også et elektronisk meldeskjema for å melde behandling av personopplysninger på siden.

I *Veileder for trygg digitalisering* fremgår det at resultatenhetsleder har ansvar for å kontrollere at opplysninger om egne behandlinger i protokollen er korrekte og at resultatenhetsledere jevnlig skal rapportere status gjennom kommunens årlige sjekkliste for internkontroll.

Revisjonen har fått tilsendt protokoll over interne og eksterne behandlingsaktiviteter tilknyttet BBSI. Eksempel på intern behandling av personopplysninger er behandling av innsynsbegjæringer og klager, innkalling til skoletannlege og innfri retten til særskilt språkopplæring. Eksempel på ekstern behandling av personopplysninger er kontantstøtteregister, fritak fra opplæring i kroppsøving og særskilt språkopplæring i grunnskolen. Den eksterne og interne protokollen har samme oppsett med ti kolonner hvor man skal fylle

[36] Allmenningen.bergen.kommune.no [lest 05.06.2019].

ut blant annet hva behandlingen gjelder, behandlingsgrunnlag, kategorier av registrerte, person-opplysninger og mottakere, samt rettslig forpliktelse.[37]

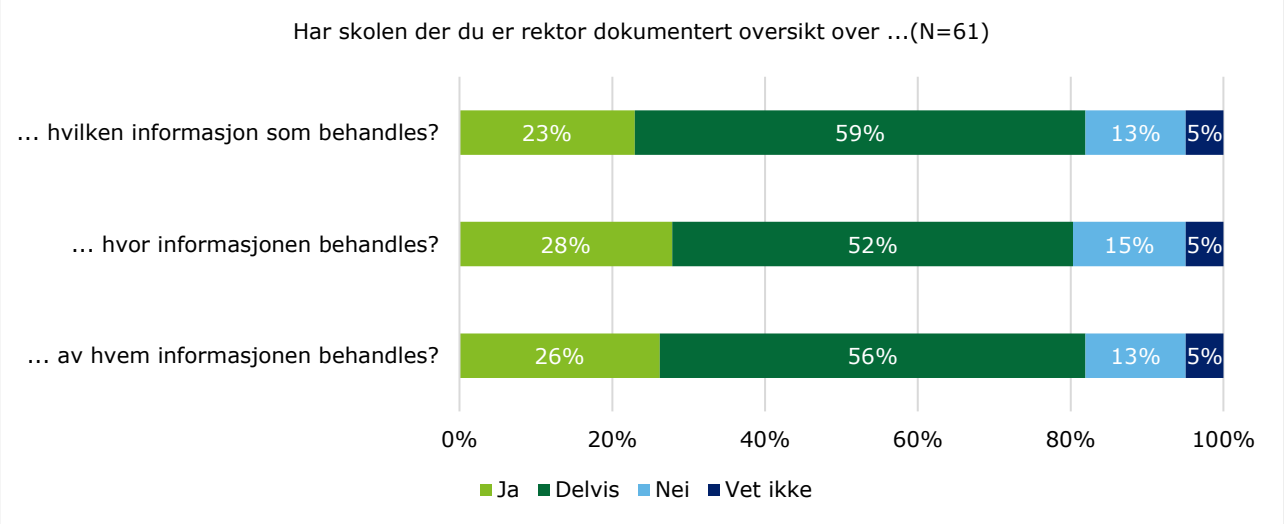
I intervju blir det fortalt at BBSI har oversikt over personopplysningene som behandles i systemene de er kjent med. På de årlige IKT-kontakt møtene blir det informert om at skolene ikke skal ta i bruk system som ikke er meldt inn til Fagavdelingen. Likevel er det flere skoler som tar i bruk systemer uten å melde fra om dette. Eksempler på dette er Klassetrivsel og SWIS, to systemer som byrådsavdelingen ikke var klar over at var i bruk, hvorav det ene (SWIS) ble stengt etter instruks fra Datatilsynet.

IKT-koordinator mener at noe av bakgrunnen for slike situasjoner oppstår er at ca. 30-40 % av skolene ikke sender representanter til IKT-kontakt møtene (se mer om IKT-kontaktene under avsnitt 3.3.9),[38] at informasjon om informasjonssikkerhet går tapt ved utskifting av stab/ledelse, og at informasjonssikkerhet historisk sett ikke har vært høyt prioritert verken i skolene eller sentralt i byrådsavdelingen.

I motsetning til tidligere, kan ikke ansatte i kommunen – og heller ikke ansatte ved skolene – installere programvare lokalt på sine PC-er uten at disse er forhåndsgodkjent. Dette har redusert risikoen for at det tas i bruk pedagogiske verktøy uten at BBSI vet om det. Likevel blir det påpekt at det nå er mange tilbydere av pedagogiske verktøy i «skyen». Bergen kommune har informert skolene om at alle systemer som skal tas i bruk må være godkjent sentralt. Likevel er det teknisk mulig for den enkelte å ta i bruk slike skybaserte tjenester. Dette har i sin tur økt risikoen for at det tas i bruk skybaserte verktøy for bruk i undervisningen, men som BBSI ikke har oversikt over.[39] Disse kan inneholde personopplysninger, noe som gjør at flere av de intervjuede ikke er trygg på at de har full oversikt over personopplysninger som behandles i skolen, og videre at det kan være leverandører der de skulle hatt databehandleravtale, uten at dette foreligger.

Rektorene fikk gjennom spørreundersøkelsen spørsmål om hvorvidt skolen har dokumentert oversikt over hvilken informasjon som behandles, hvor informasjonen behandles og av hvem informasjonen behandles:

Figur 10: Dokumentert oversikt over behandling av informasjon



[37] I protokollen over interne behandlingsaktiviteter er det lagt inn åtte kolonner som ikke er med i protokollen over eksterne behandlinger. Kolonnene har følgende kategorier: planlagte tidsfrister for sletting, beskrivelse av tekniske og organisatoriske sikkerhetstiltak, om behandlingen innebærer høy personvernrisiko, navn på databehandlere, kontaktopplysninger til behandlingsansvarlig, navn på tredjeland eller internasjonale organisasjoner som personopplysninger overføres til og nødvendige garantier ved overføring til tredjeland eller internasjonale organisasjoner.

[38] I forbindelse med høringen av rapporten opplyser kommunen at dette er en økning fra tidligere, og at fremmøte fra skolene vurderes som godt på disse møtene av pedagogisk IKT-koordinator.

[39] I forbindelse med verifiseringen opplyser kommunen at Feide for elever i undervisningen ble innført rundt 2010 slik at tilgang til programvareløsninger fra da av skulle håndteres av BBSI sentralt. Problemstillingen om bruk av skybaserte verktøy er kun mulig om en bruker en privat innlogging i skyen og at eksterne leverandører tillater dette. Kommunen har sendt informasjon til skolene om at alle systemer som skal tas i bruk må være godkjent sentralt. Revisjonen har fått tilsendt dokumentasjon på at slik informasjon er sendt.

Som fremstilt i figur 10 over svarer mellom 23 % og 28 % «ja» på de tre spørsmålene, mellom 52 % og 59 % «delvis», mellom 13 % og 15 % «nei», og 5 % «vet ikke».

Rutiner for risikovurderinger av informasjonssikkerhet

Kommunens *Reglement for trygg digitalisering* stiller krav til arbeidet med risikovurderinger:

- Den enkelte resultatenhet bør, i samråd med kommunens personvernombud, vurdere og stadfeste hva som er å betrakte som akseptabel risiko i egen resultatenhet
- Risikovurdering må dokumentere hvilke tiltak som er foreslått, planlagt og gjennomført, samt en ansvarliggjøring og oppfølgingsfrist.

Reglementet viser videre til omtale av risikovurdering på *Allmenningen*; her får man informasjon om hvordan man kan gjennomføre en risikovurdering innenfor informasjonssikkerhet og personvern, akseptkriterier, hendelser og vurdering av risiko, og hvordan man kan planlegge tiltak. Videre finner man maler og verktøy for å gjennomføre risikovurdering.

Allmenningen har også en temaside som omhandler *Vurdering av personvernkonsekvenser (DPIA)*[40] der det går frem at det skal gjennomføres en DPIA dersom det skal etableres ny behandling av personopplysninger. Det er lagt inn lenke til et skjema hvor man kan utføre en slik vurdering av behov for DPIA. I skjema skal man blant annet svare ja/nei på spørsmål om det er absolutt nødvendig å behandle personopplysninger for å nå formålet. Videre skal man svare ja/nei på 9 spørsmål for å identifisere om det er behov for DPIA. Dersom det er to eller flere «ja» på spørsmål 1-9, eller dersom behandlingen involverer innovativ bruk av ny teknologi, skal DPIA gjennomføres.

Kommunen opplyser at måten arbeidet med risikovurderinger skal bli utført i BBSI er at alle IT-tjenester og IT-løsninger skal være sentralt styrt i byrådsavdelingen, fra anskaffelse til utrulling i produksjon. Før systemer tas i bruk i produksjon, skal det gjennomføres risiko-, sikkerhets- og sårbarhetsanalyse (ROS) og eventuelt DPIA.

Videre blir det opplyst at det utarbeides tiltaksplaner som innarbeides i forkant og ved bruk av løsningene. For hvert fagsystem som skal tas i bruk i skolene utpekes det en systemkoordinator på BBSI som har ansvar for driften, herunder det sikkerhetsmessige i løsningen. Dette innebærer også manualer for bruk, opplæring og administrering av brukerkontoer og tilganger, samt samhandling med driftsleverandør i forhold til teknisk sikkerhet.

Revisjonen har fått tilsendt maler for arbeidet med ROS-analyser av digitale system på seksjon skole, blant annet mal for ROS-analyse av personopplysninger. Mal for ROS-analysen av personvernopplysninger er et regneark der det er satt opp 17 mål/krav som skal vurderes opp mot risikokriterier knyttet til sannsynlighet og konsekvens. Videre er det lagt inn et ark hvor man kan fylle inn oppsummering av ROS-analysen, samt et ark med eventuell tiltaksplan etter gjennomført analyse. Kravene som skal vurderes i analysen er blant annet integritet og konfidensialitet, formålsbegrensing, den registrertes rett til innsyn, rett til sletting av opplysninger, protokoller over behandlingsaktivitet og etterlevelse av interne krav og rutiner.

Revisjonen har videre fått tilsendt oversikt over IT-systemer og –tjenester som benyttes i skolesektoren og som eies av BBSI. I denne oversikten fremgår det at det er gjennomført ROS-analyser for åtte systemer/ tjenester og at det planlegges eller er behov for ROS-analyser av ytterligere fem system/tjenester.

ROS-analysene som var gjennomførte ved BBSI tidlig i revisjonsperioden var Azure Active Directory, BK360, eFeide, Google Gsuite for Education, Klassetrivsel, Microsoft Office 365, Spekter og Vigilo. I to av systemene, Klassetrivsel og Spekter, ble det vurdert at det var behov for at ROS-analysen blir etterfulgt av en DPIA. Etter gjennomført DPIA av Klassetrivsel stengte kommunen midlertidig bruk av programmet.[41]

---

[40] *Data Protection Impact Assessment*, forkortet DPIA, og oversatt til vurdering av personvernkonsekvenser.

[41] I forbindelse med verifiseringen av rapporten opplyser kommunen at BBSI også har gjort ROS-analyser av følgende systemer: AV1, Brief-P, CBCL - Child Behavior Checklist, Creaza, Conexus Engage, HK Oppvekst (PPT), Innblikk, UEVO-studien, MultiSmart Øving og Mittyrke.no. Videre opplyser kommunen at DPIA er gjennomført på behandlingsaktiviteten «trivselsundersøkelser i skolen», som benytter «Spekter» og «Klassetrivsel» som understøttende IT-løsninger. I tillegg opplyser kommunen at de på bakgrunn av Datatilsynets «Vedtak om pålegg -

I flere av risikovurderingene revisjonen har fått tilsendt fremgår det hvem som har vært involvert i prosessen. Gjennomgående har dette vært systemkoordinatorer og IKT-koordinatorer.

Systemkoordinatorene forteller i intervju at ROS-analysene ble gjennomført vinteren/våren 2018-2019 på grunn av ny personopplysningslov, og at man før dette ikke hadde utført ROS-analyse på annet enn ett system.[42] Etter gjennomgangen med ROS i 2018/2019 har man på seksjonen bedre oversikt over systemene som benyttes i skolesektoren.[43]

Mot slutten av revisjonsperioden kom det frem opplysninger om at det var avdekket brudd på informasjonssikkerheten i Vigilo knyttet til uautorisert innsyn i konfidensielle opplysninger. Risikoen for at et slikt informasjonssikkerhetsbrudd kunne finne sted var identifisert og vurdert i kommunens ROS-analyse av Vigilo. Det ble i risikoanalysen pekt på at treghet i oppdateringene i kommunens interne kopi av folkeregisteret kunne føre til at foresatte fradømt foreldreretten fikk tilgang til informasjon om barnet sitt når informasjon derfra ble tatt i bruk i Vigilo. Som risikoreduserende tiltak hadde derfor BBSI allerede som rutine å manuelt redigere relevante data fra kommunens kopi av folkeregisteret. I tillegg står det oppført som nytt risikoreduserende tiltak at kommunen skal avklare muligheter med leverandøren for bruk av kommunens kopi av folkeregisteret, uten at hva dette skulle innebære er nærmere spesifisert.

Av organisatoriske og tekniske årsaker kunne ikke opplysninger om nye elever for skoleåret 2019-2020 importeres i Vigilo fra kommunen sin egen kopi av folkeregisteret, men måtte hentes fra det sentrale folkeregisteret. Før innlesing av opplysninger derfra, stilte kommunen spørsmål til leverandøren om hva som var risikoen knyttet til operasjonen. Revisjonen får opplyst at svaret fra Vigilo ble tolket dithen at innlesingen ikke innebar noen risiko. Kommunen har i oppfølgingssamtaler med revisjonen vært åpen på at det her kan ha oppstått misforståelser.[44]

I forbindelse med verifiseringen av rapporten, opplyser kommunen at leverandøren av Vigilo i et foredrag før sommeren 2019 påpekte den overnevnte risikoen, men at dette fremgår ikke i referat fra det aktuelle møtet eller i rutiner eller ROS-analyser senere distribuert fra leverandøren.

Ved innlesing av opplysninger fra det sentrale folkeregisteret til Vigilo, ble foreldrerelasjonen til alle elever – både nye og gamle elever – importert, uavhengig av foreldreansvar. Da systemet ble tatt i bruk, ble det oppdaget at meldinger til foresatte ble automatisk sendt til alle som står registrert som foreldre til barnet i det sentrale folkeregisteret, også de som ikke har foreldreansvar. Disse meldingene inneholdt informasjon om Vigilo og skolen til barnet. Innlogging i Vigilo gir tilgang til barnets navn, skole, klasse, navn på ansatte ved barnets skole, samt navn på andre foresatte knyttet til barnet.

Selv om risikoen for at foresatte uten foreldreansvar fikk tilgang til informasjon om barnet var identifisert og vurdert i ROS-analysen av Vigilo, var den *identifiserte* årsaken i ROS-analysen – at dette kunne skje som følge av treghet i oppdateringene i kommunens interne kopi av folkeregisteret – ikke dekkende for den *faktiske* årsaken til informasjonssikkerhetsbruddet – altså at det ved innlesing av opplysninger fra det sentrale folkeregisteret til Vigilo ble alle foreldrerelasjoner til alle elever importert, uavhengig av foreldreansvar. Følgelig var iverksatte risikoreduserende tiltak – som å manuelt «vaske» kommunens lokale kopi av folkeregisteret – ikke tilstrekkelige til å forhindre det inntrufne (se også avsnitt 4.3.1).

I forbindelse med verifiseringen av rapporten fremholder kommunen at ROS-analysen ikke var mangelfull på tidspunktet den ble gjennomført (april 2019), da innlesning av data fra det sentrale folkeregisteret ikke var en aktuell rutine på tidspunktet. I kommunen sitt *Svar på krav om tilsvar etter melding om avvik i Vigilo* til Datatilsynet i november,[45] fremgår det at kommunen ikke gjennomførte ROS-analyser eller

---

Arendal kommune - Behandling av personopplysninger i kartleggingsverktøyet Spekter», har besluttet å gjennomføre ny ROS og DPIA på bruk av disse og eventuelle tilsvarende verktøy, som en prioritert aktivitet i november-desember 2019.

[42] Det fremgår i intervju med systemkoordinatorene at det ble gjennomført et møte med forhenværende Personvernombud i kommunen i august 2018 for å ha en gjennomgang på hvordan å utføre en vurdering av personvernkonsekvenser (DPIA). Dette var på daværende tidspunkt et nytt område også for Personvernombudet. Systemkoordinatorene gjennomførte første DPIA i kommunen sammen med Personvernombudet.

[43] Det har også i perioden vært innleid en ekstern konsulent som har vært til god hjelp i å få på plass en oversikt.

[44] Revisjonen har fått tilsendt kopi av lynmeldingskorrespondanse mellom kommunen og leverandøren.

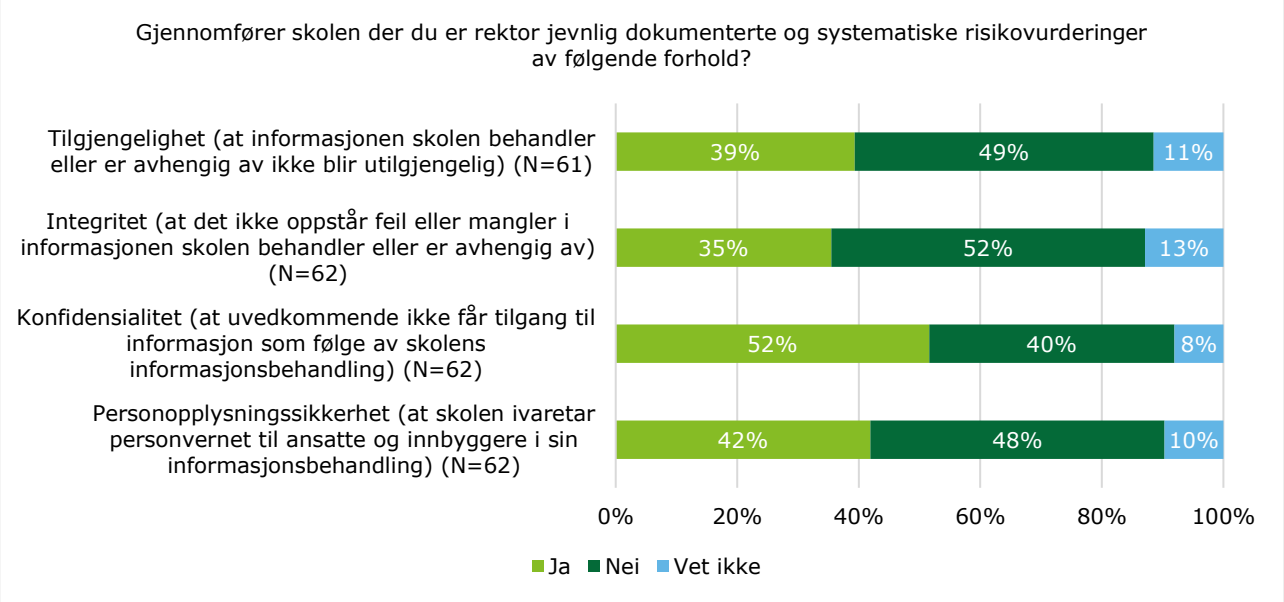
[45] *Svar på krav om tilsvar etter melding om avvik i Vigilo*, 11. november 2019.

personvernkonsekvensvurderinger i forbindelse med at kommunen hentet personopplysninger fra det sentrale folkeregisteret.

Kjennskap til ansvar for risikovurderinger

Rektorene som deltok i spørreundersøkelsen fikk spørsmål knyttet til om de gjennomfører risikovurderinger. Svarene er fremstilt i figur 11 under:

Figur 11: Gjennomføring av risikovurderinger i skolene



Som vist i figuren, svarer 40 % av respondentene «nei» på spørsmålet om de gjennomfører jevnlige dokumenterte og systematiske risikovurderinger av konfidensialitet, mens mellom 48 % og 52% svarer «nei» på spørsmål om det blir gjennomført risikovurderinger av personopplysningssikkerhet, integritet og tilgjengelighet. 13 % av rektorene som deltok i spørreundersøkelsen vet ikke om det blir gjennomført risikovurderinger av integritet, mens mellom 8 % og 11 % svarer «vet ikke» på spørsmål om skolen gjennomfører risikovurderinger av tilgjengelighet, konfidensialitet og personopplysningssikkerhet.

De som svarte «nei» på spørsmålene som er gjengitt i figur 11 fikk oppfølgingsspørsmål om hva som er bakgrunnen for at det ikke er utført risikovurderinger innen de ulike områdene. På dette svarte mellom 15 og 18 rektorer at de «ikke har vært klar over at det er forventet at dette skal gjøres», mens mellom seks og åtte respondenter svarte at de «ikke har hatt tilgang nødvendige verktøy for å gjøre dette», og mellom syv og ni oppgir at de «ikke har hatt kompetanse om hvordan man gjør dette». Videre viser mellom seks og åtte rektorer til at de ikke har hatt tid til å gjennomføre risikovurderinger innenfor de fire ulike områdene.[46]

Rutine for håndtering av avvik

Det blir i *Reglement for trygg digitalisering* slått fast at all behandling av informasjon som bryter, eller kan komme til å bryte med kommunens sikkerhetsmål, skal rapporteres som avvik. Videre fremgår det at avvik skal meldes i kommunes gjeldende avvikshåndteringssystem og følges opp i samråd med personvernombudet for å avgjøre om avviket skal meldes til Datatilsynet.

[46] Det var òg mulig å begrunne manglende risikovurderinger i et fritekstfelt. Av dem som benyttet seg av denne muligheten, kom det blant annet svar om at de er nye i rollen som rektor, eller at de ikke har tenkt over dette. Én respondent svarer at det ikke har vært fokus på systematiske risikovurderinger på området og at vedkommende har antatt at dette området er ivaretatt ved å bruke prosedyrene som for eksempel foreligger i BK360. En annen svarer at når det gjelder risikovurderinger av personopplysningssikkerhet og er de underlagt kommunens system, og derfor ikke trenger eget på hver enhet.

Kommunen har en *Overordnet rutine for håndtering av avvik som gjelder personvern og informasjons-sikkerhet*[47] som er felles for alle byrådsavdelingene i kommunen. I denne fremgår blant annet avdeling for personvern og informasjonssikkerhets-, enhetsleders- og ansattes ansvar for melding av avvik, samt saksgang ved melding av avvik:

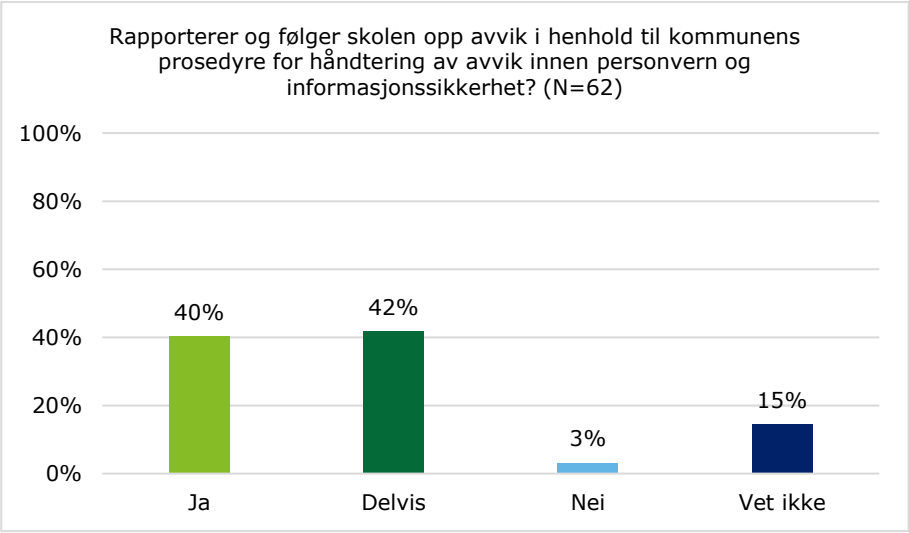
Tabell 7: Internt ansvar for melding av avvik

Rolle	Ansvar
Avdeling for personvern og informasjonssikkerhet	• Gi råd og veiledning til enhetsledere for oppfølgning av avvik • Rapportere avvik, med konsekvenser for personvernet, til Datatilsynet innen 72 timer fra avviket skjedde
Enhetsledere	• Fastsette krav til konfidensialitet, integritet og tilgjengelighet, og kommunisere disse i linjen • Iverksette umiddelbare tiltak ved avvik • Snarest, og innen 48 timer fra avviket skjedde, rapportere avvik til avdeling for personvern og informasjonssikkerhet • Systematisk gjennomgang av meldte avvik
Ansatte	• Kjenne til interne rutiner for avvikshåndtering i enheten • Melde avvik til sin enhetsleder, snarest etter de ble oppdaget • Vurdere, og iverksette, egne strakstiltak

På *Allmenningen* er det lagt inn informasjon om avvikshåndtering knyttet til personvern og informasjonssikkerhet.[48] Det fremgår her hva som regnes som et avvik, hva som kan inngå i melding av uønsket hendelse og at dette skal meldes via BK Kvalitet, samt hva som er prosess for oppfølging av denne typen avvik i kommunen. Det er videre lagt inn lenke til å melde inn avvik via kvalitetssystemet og lenke til den overordnede rutinen for avvik.

Rektorene som deltok i spørreundersøkelsen fikk spørsmål om skolen sin håndtering av avvik:

Figur 12: Rapportering og oppfølging av meldte avvik



[47] Overordnet rutine for håndtering av avvik som gjelder personvern og informasjonssikkerhet. Revisjonsdato 31.01.2018. Gyldig til 28.02.2019.
[48] https://allmenningen.bergen.kommune.no/ansatthjelpen/virksomhetsstyring/internkontroll/informasjonssikkerhet-og-personvern/avvikshandtering-personvern-og-informasjonssikkerhet

Som vist i figur 12, svarer litt færre «ja» (40 %) enn «delvis» (42 %) på spørsmålet, mens 3 % svarer «nei» og 15 % «vet ikke» (se avsnitt 6.2 om de ansattes kjennskap til avviksrutiner knyttet til informasjonssikkerhet, samt i hvor stor grad de melder avvik og om de meldte avvikene blir fulgt opp).

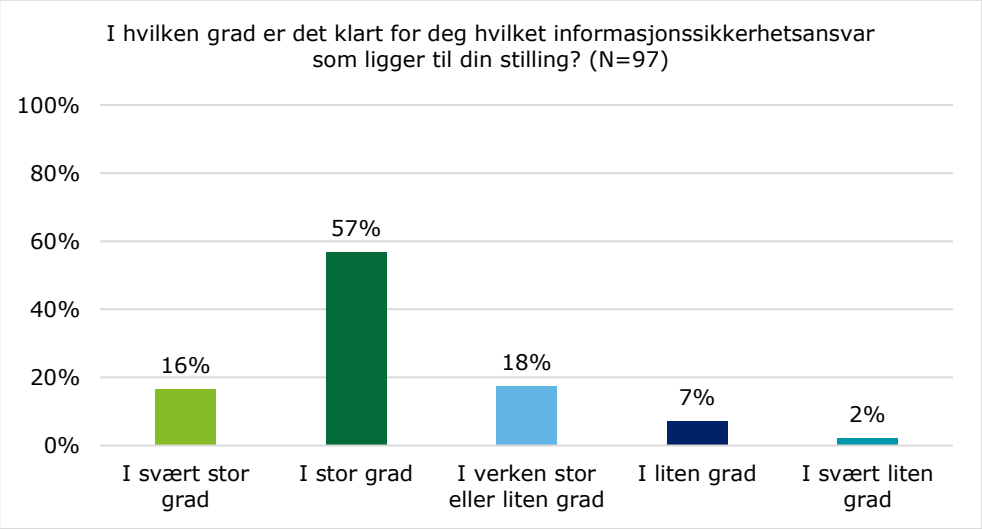
Revisjonen har ikke gjort undersøkelser knyttet til avvikshåndtering blant enhetsledere. Likevel registrerer vi at en rektor fikk melding om informasjonssikkerhetsbruddet i Vigilo,[49] uten at det på den bakgrunn ble iverksatt tiltak. Kommunen opplyser i forbindelse med verifiseringen av rapporten at «saken ble behandlet etter gjeldende rutine da den oppstod», og at det senere er kommet på plass nye rutiner med hensyn til å melde inn avvik i avvikssystemet. Videre opplyser kommunen at de ble gjort oppmerksom på avviket i form av spørsmål fra en skole via SMS, men at det ble oppfattet som en enkelthendelse og ikke en systematisk feil. SMS ble svart ut med henvisning til en faghjelp/rutine med veiledning til å oppklare hvem som har rett på informasjon. Kommunen opplyser videre at meldingen fra skolen var et viktig bidrag når saken først ble meldt 3. september 2019 da det førte til at man raskere kunne konkludere/fastsette årsak.

3.3.8 Ansatte

Som nevnt over, viser *Reglement for trygg digitalisering* til de ansattes informasjonssikkerhetsansvar, mens det i *Oppdragsbeskrivelsen for alle ansatte for akseptabel bruk av IKT*[50] stilles krav til hvordan IKT-utstyr og –systemer skal benyttes. Oppdragsbeskrivelsen viser også til prosedyrer, retningslinjer, sjekklister og utfyllende informasjon knyttet til informasjonssikkerhet på *Allmenningen*.

De ansatte i skolesektoren som deltok i spørreundersøkelsen fikk spørsmål om i hvilken grad informasjons-sikkerhetsansvaret som ligger til stillingen deres oppleves som klart. [51] Svarene fremgår i figuren under:

Figur 13: Tydelig informasjonssikkerhetsansvar



Figur 13 viser at langt de fleste svarer at informasjonssikkerhetsansvaret som ligger til deres stilling enten «i svært stor grad» (16 %) eller «i stor grad» (57 %) er klart, og at til sammen 9 % opplever ansvaret som «i liten grad» (7 %) eller «i svært liten grad» (2 %) er klart.

3.3.9 Andre roller i skolesektoren knyttet til informasjonssikkerhet

Områdeledere

På organisasjonskartet som var gjeldende frem til omorganiseringen av byrådsavdelingen fra 1. juli 2019 var områdelederne plassert i direkte linje under kommunaldirektøren, og var nærmeste overordnede til enhetslederne i barnehage og skole. Skolene (og barnehagene) er delt inn i fire ulike byområder: byområde sør (Fana/Ytrebygda), byområde sentrum (Bergenhus/Årstad), byområde nord (Arna/Åsane) og byområde

[49] Se *Rutiner for risikovurderinger av informasjonssikkerhet* (under avsnitt 3.3.7) og avsnitt 4.3.1.
[50] *Oppdrag for alle ansatte for akseptabel bruk av IKT*. Ikke datert
[51] Spørsmålet ble stilt til de ansatte som oppgav at de ikke var resultatenhetsleder eller systemeier

vest (Fyllingsdalen/Laksevåg) og hvert byområde har hver sine tilknyttede områdeledere: en områdeleder for skolene i byområde nord, en for byområde sentrum, en for byområde vest og to for byområde sør.[52]

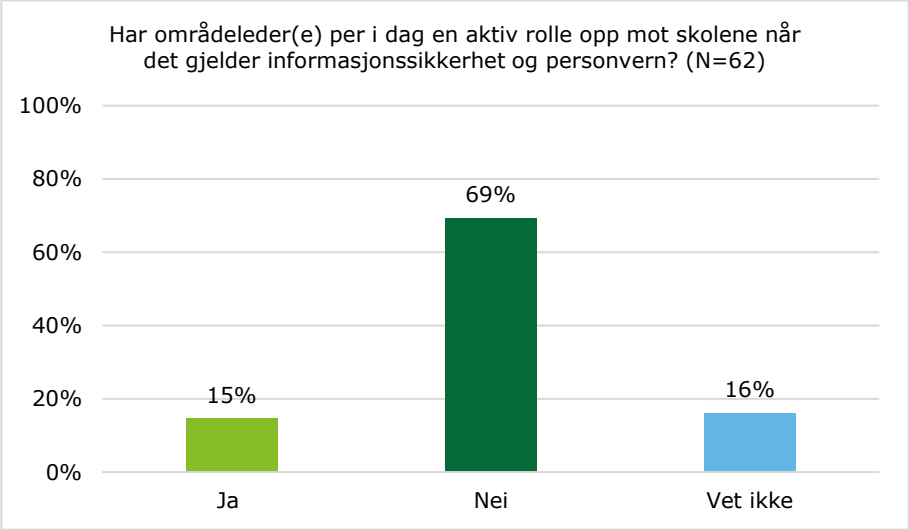
Områdelederne arrangerte blant annet områdemøter (tidligere kalt rektormøter) og gjennomførte ledersamtaler med én og én rektor. Oppgavene til områdelederne inkluderte videre å skrive lederavtaler med rektorene, samt følge opp HMS-arbeid og avviksrapportering.

Som vist under avsnitt 2.1 er det planlagt at områdelederne etter omorganiseringen av BBSI skal få ansvar for å sikre at skolene etterlever informasjonssikkerheten på vegne av etatslederen. I intervju blir det påpekt at områdelederne på revisjonstidspunktet ikke har noen reell rolle for informasjonssikkerhet i skolene, og at det i praksis ikke har vært noe mellomledd mellom kommunaldirektøren og rektorene når det gjelder informasjonssikkerhet.[53] Likevel blir det vist til at noen områdeledere er interessert i informasjonssikkerhet, og tar opp temaet på områdemøter.

Systemkoordinatorene forteller at de noen ganger kontakter områdelederne dersom det oppstår problemstillinger i forbindelse med rektors utføring av oppgaver på systemområdet. Dersom koordinatorene ikke får gjennomslag hos rektorer kontakter de aktuell områdeleder og ber vedkommende ta dette opp med vedkommende rektor. Det kommer frem at det i disse tilfellene har vært eksempel på at heller ikke områdelederne er bevisste på viktigheten av informasjonssikkerhet for eksempel i form av tilgangsstyring.

På spørsmål om områdelederne har en aktiv rolle opp mot skolene når det gjelder informasjonssikkerhet og personvern fordeler svarene fra rektorene seg som vist i figur 14:

Figur 14: Områdeledere og informasjonssikkerhet



Som fremstilt i figuren, svarer 69 % «nei» på spørsmålet om områdelederne har en aktiv rolle opp mot skolene når det gjelder informasjonssikkerhet, mens 16 % svarer «vet ikke». De 15 % som svarte «ja» på spørsmålet fikk et oppfølgingsspørsmål der de kunne forklare kort hvilken rolle områdelederne har opp mot

[52] Oversikten er pr. juli 2019 og er hentet fra Allmenningen: https://allmenningen.bergen.kommune.no/faghjelpen/barnehage-og-skole/forvaltning-og-juss/oversikt-omradeledere-skole-pr-juli-2019

[53] Kommunen viser i forbindelse med verifiseringen av rapporten til fagfullmaktene av 2. februar 2017, punkt 1 om områdelederne og fagdirektør for barnehage og skole sine delegerte fullmakter, som sier at disse skal «se til at skoler, barnehage og PPS gir tjeneste i henhold til gjeldende lov- og regelverk, vedtatte økonomiske rammer og øvrige kommunale styringsdokument og føringer». Informasjonssikkerhet er ikke særskilt nevnt i fagfullmaktene.

skolene når det gjelder informasjonssikkerhet. Av de åtte som svarer på dette spørsmålet oppgir fire at områdekontaktene følger opp skolene når det gjelder rutiner.[54]

IKT-kontakt

Kommunen opplyser at det utenom de overordnede rollene som er beskrevet i styringssystemet for personvern og informasjonssikkerhet er etablert en ordning med strategisk IKT-gruppe og IKT-kontakter i skolene[55] som har informasjonssikkerhetsansvar innenfor BBSI. Kommunen opplyser følgende om den strategiske IKT-gruppen:

> sentrale ressurser med særlig kompetanse innen systemsikkerhet utgjør avdelingens strategiske IKT-gruppe. Gruppens hensikt er å fremskaffe beste mulig beslutningsgrunnlag for viktige og tverrsektorielle beslutninger.

I intervju blir det fortalt at det ikke lenger er et krav at man har IKT-kontakt på skolene. For omtrent syv år siden tildelte byrådsavdelingen noen øremerkede stillingsprosenter til skolene som skulle brukes for å ivareta IKT-kontaktoppgaver. I dag er det opp til hver enkelt skole om de ønsker å ha IKT-kontakt; noen har for eksempel en avdelingsleder som ivaretar denne rollen mens på andre skoler er det rektor som har denne rollen.

Pedagogisk IKT-koordinator er kontaktperson for IKT-kontaktene, og forteller at det er behov for flere ressurspersoner knyttet til IKT i de enkelte skolene. Han forteller at det for eksempel er behov for lokale ressurspersoner som kan hjelpe til når skolene innfører nye verktøy som digital tavle og Chromebooks. Det fremgår i intervju at signalet fra etatsdirektøren er at lærerne selv skal bli kompetente i programmene og verktøyene som blir benyttet.

Pedagogisk IKT-koordinator forteller videre at han opplever et stadig større behov for kommunikasjon mellom pedagogisk IKT-koordinator og IKT-kontaktene ved skolene. Det er løpende dialog mellom partene, og pedagogisk IKT-koordinator anslår at han tidligere mottok mellom fire og seks e-poster fra IKT-kontakter i løpet av en uke, mens tilfellet nå er at han får samme andel e-poster i tillegg til mange telefoner. Samtidig fremgår det at skolene tidligere kontaktet pedagogisk IKT-koordinator med spørsmål knyttet til problemstillinger med programmene, men at skolene i stor grad nå kontakter Helpdesk med denne typen forespørsler.

Det fremgår at det gjennomføres ett møte i året der IKT-kontaktene i skolene samles.[56] Hvert møte blir avholdt tre ganger for å fordele deltakerne. Det er ikke alle skolene som har IKT-kontakt, og dermed ikke alle skolene som sender representanter til disse møtene. Tema for IKT-kontaktmøtene er læring og pedagogikk og møtene er lagt opp som dialogmøter.

Det fremgår i intervju at det i forkant av IKT-kontaktmøtet blir lagt ut en kort agenda med informasjon om tema for møtet. Det blir videre fortalt at man ikke skriver referat fra møtene, men at eventuelle slides fra foredrag eller lenker til informasjon blir lagt ut via *itslearning*.[57] I tillegg samskriver deltakerne i IKT-kontaktmøtene notater via et dokument som ligger i skytjenesten. Når alle de tre møtene (som er helt like) er gjennomført blir det lagt ut et felles notat etter samsskrivingen som er tilgjengelig for alle deltakerne.

Revisjonen har fått tilsendt agenda for møter arrangert i 2016, 2017 og 2018, samt samskrivingsnotatene fra de samme møtene. Det fremgår ikke av agenda eller notatene at informasjonssikkerhet og/eller systemsikkerhet har vært tema på møtene i 2016 og 2017. I agenda for møtet som ble gjennomført høsten 2018 fremgår det at det at pedagogisk IKT-koordinator har hatt en 20 minutters sekvens som blant annet har hatt GDPR og bestillinger av tilganger og apper som tema.[58]

---

[54] Én av respondentene legger til at områdeleder følger opp rektor i virksomhetsstyringssystemet *Corporater* når det gjelder «rutiner og planer skolen skal ha i henhold til informasjonssikkerhet og/eller personvern». Videre fremgår det at områdeledere blant annet har gitt informasjon om sikkerhet knyttet til system og programmer på områdemøter.
[55] Kommunen opplyser at IKT-kontakten skal «ivareta nødvendig kontakt mellom Fagavdelingen, og deltar i opplæring av nye systemer, nytt utstyr med mer».
[56] Dette møtet blir benevnt som både IKT-kontaktmøte og dialogmøte.
[57] Det er et eget fag i *itslearning* som heter «IKT-kontakt». Det hender at pedagogisk IKT-koordinator legger ut relevant informasjon til IKT-kontaktene i denne modulen.
[58] I forbindelse med verifiseringen kommenterer kommunen at personvern og IKT-sikkerhet har vært en del av informasjonen fra IKT-koordinator på IKT-kontaktmøtene fra 2016. Det har vært lagt inn som en egen fane i bloggen

3.4 Vurdering

Gjennom styringssystemet for personvern og informasjonssikkerhet og tilhørende oppdragsbeskrivelser, mandater og veiledere, har Bergen kommune skriftliggjort ansvar og oppgaver knyttet til informasjonssikkerhet. Styringssystemet gjelder for hele kommunen. I de ulike dokumentene som inngår i styringssystemet fremgår det hvilket ansvar som påhviler flere ulike roller, samt hvilke oppgaver de skal utføre for å sikre god informasjonssikkerhet i kommunen; behandlingsansvaret er tydelig lagt til kommunaldirektørene, og både informasjonssikkerhetsansvaret og -oppgavene til resultatenhetsledere, systemeiere og ansatte er skriftliggjort.

Overordnet finner revisjonen at rolle- og ansvarsfordelingen knyttet til informasjonssikkerhet i byrådsavdelingen og i skolesektoren verken oppleves som tydelig eller som hensiktsmessig organisert. I praksis har ikke delegering internt i byrådsavdelingen fungert i praksis på dette området, noe som betyr at det reelt sett ikke har vært noe koordinerende eller styrende ledd mellom kommunaldirektøren og rektorene når det gjelder informasjonssikkerhet. Revisjonen er oppmerksom på at det som et ledd i omorganiseringen i byrådsavdelingen er etablert en seksjon for HR, digitalisering og virksomhetsstyring som blant annet skal bedre ivareta informasjonssikkerhetsområdet i tett samarbeid med andre sentrale IKT-faglige miljø i kommunen, samt at det er opprettet en stilling som rådgiver for informasjonssikkerhet.[59]

Når det gjelder den praktiske rolle- og ansvarsfordelingen sentralt i skolesektoren, finner revisjonen blant annet at det har vært en IKT-koordinator som i lengre tid har tatt og hatt et ansvar for informasjonssikkerheten. Dette ansvaret har ikke vært formalisert, og IKT-koordinatorrollen inngår ikke i kommunens styringssystem. Videre opereres det i skolesektoren med en systemkoordinatorrolle som heller ikke er å finne i kommunens styringssystem. Systemkoordinatorene har fått delegert ansvar for informasjonssikkerheten i systemene fra systemeier, uten at dette ansvaret er skriftliggjort. Systemeierrollen har på sin side ikke hatt eller ivaretatt noe informasjonssikkerhetsansvar i skolesektoren. Revisjonen registrerer òg at hvem som faktisk er systemeier for de ulike systemene i skolesektoren ikke er tydelig.

Revisjonen merker seg videre at de to rollene med et praktisk om enn uformelt informasjonssikkerhetsansvar – IKT-koordinator og systemkoordinator – bare delvis forholder seg til kommunens styringssystem for informasjonssikkerhet. I intervju blir det vist til at det i stedet er retningslinje for IT-sikkerhet fra 2002 som blir lagt til grunn.

Basert på det overstående, er det revisjonen sin vurdering at informasjonssikkerhetsarbeidet sentralt i skolesektoren i Bergen kommune preges av en uformell rolle- og ansvarsdeling, noe som gir økt risiko for uklarheter og manglende oppfølging av informasjonssikkerhetsarbeidet, med tilhørende risiko for brudd på informasjonssikkerheten.

Informasjonssikkerhetsbruddet knyttet til Vigilo viser at slik risiko har gjort seg gjeldende i kommunen. Avviket indikerer at ansvar og oppgaver knyttet informasjonssikkerhet ikke i tilstrekkelig grad er ivaretatt i byrådsavdelingen. Selv om risikoen for at det inntrufne kunne skje ble identifisert og vurdert i ROS-analysen av Vigilo, og det ble iverksatt risikoreduserende tiltak, var den *identifiserte* årsaken til risikoen ikke dekkende for den *faktiske* årsaken til informasjonssikkerhetsbruddet. Følgelig var ikke iverksatte risikoreduserende tiltak tilstrekkelige til å forhindre det inntrufne. ROS-analysen var med andre ord mangelfull, noe som ikke ble avdekket før det forekom et faktisk informasjonssikkerhetsbrudd.

Revisjonen registrerer i denne forbindelse at kommunen fremholder at ROS-analysen ikke var mangelfull på tidspunktet den ble gjennomført, da det å importere opplysninger direkte fra det sentrale folkeregisteret ikke var rutine på tidspunktet. Revisjonen merker seg videre at kommunen i sitt tilsvar til Datatilsynet vedgår at det skulle vært gjennomført en egen ROS-vurdering og personvernkonsekvensvurdering før det ble hentet inn personopplysninger fra det sentrale folkeregisteret, noe som altså ikke var gjort. Basert på dette er det revisjonen sin vurdering at ansvar og oppgaver knyttet til informasjonssikkerhet ikke i

---

IKT-koordinator som ble brukt til å informere og vise til deltakerne (https://ikt-koordinator.blogspot.com/). Bloggen har blitt oppdatert årlig og referert, vist og delt på disse møtene. Videre viser kommunen til at det flere ganger er sendt ut e-post og notater om at det enkelte tjenestested ikke kan anskaffe datasystem uten å klarere dette med Fagavdelingen.

[59] Stillingen var på revisjonstidspunktet ikke besatt, men kommunen viser til at de har leid inn ekstern hjelp med relevant kompetanse fra januar 2019 for å arbeide på dette feltet.

tilstrekkelig grad er ivaretatt i byrådsavdelingen, og at det som en følge av dette er en vedvarende risiko for informasjonssikkerhetsbrudd i skolesektoren.

Svarene i spørreundersøkelsen som gikk til kommunens rektorer, underbygger videre inntrykket av utydeligheter knyttet til rolle- og ansvarsdeling knyttet til informasjonssikkerhet. Kun én av tre av rektorene som svarte på spørreundersøkelsen, svarer «ja» på spørsmål om det er en klar rolle- og ansvarsdeling med hensyn til informasjonssikkerhet mellom byrådsavdelingen og skolen; 37 % svarer «nei» på spørsmålet, og 30 % «vet ikke». Revisjonen vil i denne forbindelse understreke at rektorene som resultatenhetsledere er tildelt en sentral rolle i styringssystemet for informasjonssikkerhet og personvern i kommunen, og at det følgelig er viktig at rolle- og ansvarsdelingen mellom skolene og byrådsavdelingen er tydelig og avklart. Utydelig rolle- og ansvarsdeling øker risikoen for at oppgaver og myndighetsområder knyttet til informasjonssikkerhet ikke ivaretas, med tilhørende risiko for brudd på informasjonssikkerheten.

Funn fra spørreundersøkelsen indikerer at også denne risikoen har gjort seg gjeldende. For selv om svarene fra til sammen 92 % av rektorene tyder på at informasjonssikkerhetsansvaret som påhviler dem oppleves som tydelig, svarer om lag halvparten at de ikke har eller ikke vet om de har lest sentrale styringsdokumenter og veiledninger for informasjonssikkerhet. Det er derfor ikke overraskende at svarene i spørreundersøkelsen avdekker at oppgaver som påhviler rektorene som resultatenhetsledere bare delvis blir gjennomført; flertallet av dem har enten ikke eller har bare delvis dokumentert oversikt over *hvem* som behandler *hvilken* informasjon *hvor* på skolen, rundt halvparten har ikke eller vet ikke om de har gjennomført risikovurderinger av tilgjengelighet, integritet, konfidensialitet og personopplysningssikkerhet, og svarene viser videre at rektorenes avvikshåndtering bare delvis blir ivaretatt som forutsatt. Vesentligheten ved sistnevnte moment understrekes av at informasjonssikkerhetsbruddet i Vigilo var kjent i organisasjonen flere dager før det ble håndtert som et faktisk informasjonssikkerhetsavvik.

Også de ansatte svarer i overveiende grad at eget informasjonssikkerhetsansvar er tydelig, men som vil vises i senere kapitler, avviker også deres informasjonssikkerhetspraksis fra regler og prosedyrer nedfelt i kommunens styringssystem.

Det kommer òg frem i undersøkelsen at det er usikkerhet knyttet til om og i hvilken grad områdelederne i skolesektoren per i dag har en rolle opp mot skolene når det gjelder informasjonssikkerhet. Revisjonen registrerer at områdelederne i fagfullmaktene fra 2017 var pålagt å «se til at skoler, barnehage og PPS gir tjeneste i henhold til gjeldende lov- og regelverk, vedtatte økonomiske rammer og øvrige kommunale styringsdokument og føringer». Revisjonen merker seg at det ikke står noe om informasjonssikkerhet i de nevnte fagfullmaktene. Sett i sammenheng med usikkerheten knyttet til områdeledernes informasjons-sikkerhetsrolle som kommer fram i undersøkelsen, mener revisjonen det ikke har vært tilstrekkelig tydelig informert om og hvilket ansvar som faktisk påhvilte områdelederne med hensyn til informasjonssikkerhet. Revisjonen er for øvrig oppmerksom på at områdelederne er tiltenkt en informasjonssikkerhetsrolle i den nye organiseringen. Dette var på revisjonstidspunktet ikke effektuert.

Endelig registrerer revisjonen at det på den ene siden fremholdes at skolenes IKT-kontakter og strategisk IKT-gruppe skal ivareta et informasjonssikkerhetsansvar i skolene, mens det på den andre siden kommer frem at ikke alle skolene har en slik IKT-kontakt, og videre at IKT-kontaktenes ansvar i praksis i liten grad er knyttet til informasjonssikkerhet.

Oppsummert er det revisjonen sin vurdering at det i skolesektoren ikke er etablert klare rutiner og ansvarsforhold med hensyn til informasjonssikkerhet, og videre at det som er etablert av rutiner og ansvarsforhold delvis avviker fra kommunens styringssystem for informasjonssikkerhet.

Revisjonen er oppmerksom på at det er relativt kort tid siden gjeldende styringssystem for personvern og informasjonssikkerhet ble utarbeidet og implementert i kommunen, og videre at BBSI nylig er omorganisert. Dette er begge momenter som kan være med å forklare at rutiner og ansvarsforhold i skole-sektoren når det gjelder informasjonssikkerhet ikke fremstår som entydige eller klare. Revisjonen ser det i den sammenheng som positivt både at det er opprettet en stilling som informasjonssikkerhetsrådgiver i

skolesektoren,[60] samt at områdelederne i ny organisering er tiltenkt en rolle for å legge til rette for at skolene etterlever styringssystemet for informasjonssikkerhet og personvern.

Revisjonen vil likevel understreke viktigheten av å etterleve kommunens styringssystem og tilhørende reglement, oppdragsbeskrivelser mm.

[60] Stillingen var på revisjonstidspunktet ikke besatt, men kommunen viser til at de har leid inn ekstern hjelp med relevant kompetanse fra januar 2019 for å arbeide på dette feltet.

4. Konfidensialitet

4.1 Problemstilling

I dette kapittelet vil vi svare på følgende problemstilling med underproblemstillinger:

Har skolesektoren etablert rutiner for sikring av konfidensialitet, og etterleves disse?

Under dette:

a) Hindre uautorisert innsyn i konfidensielle opplysninger
b) Sikker sone for lagring av konfidensielle opplysninger
c) Kryptering av konfidensielle opplysninger

4.2 Revisjonskriterier

Å sørge for *konfidensialitet* innebærer å hindre ikke-autorisert innsyn i informasjon som ikke skal være tilgjengelig for alle.

Personvernforordningen artikkel 32 nr. 1 stiller krav om informasjonssikkerhet ved behandling av personopplysninger. Kravene som blir stilt er at man skal sette i verk egnede tekniske og organisatoriske tiltak basert på risikovurderinger for å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene. Tiltak som også blir nevnt under artikkel 32 nr. 1 er pseudonymisering og kryptering av personopplysninger og evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse.

Se vedlegg 3 for utfyllende revisjonskriterier.

4.3 Hindring av uautorisert innsyn i konfidensielle opplysninger

4.3.1 Datagrunnlag

Retningslinjer og rutiner

De mest sentrale beskrivelsene av ansvar og rutiner knyttet til å hindre uautorisert innsyn i konfidensielle opplysninger i kommunen fremgår i *Reglement for trygg digitalisering*, *Oppdragsbeskrivelse for resultatenhetsledere* og *Oppdragsbeskrivelse for akseptabel bruk av IKT*.

Reglementet for trygg digitalisering definerer fire overordnete sikkerhetsmål som blant annet omhandler tilgang til informasjon (se tabell 2 på side 15). Reglementet viser videre til at det er resultatenhetsleders ansvar å sørge for at kommunens styrende dokumenter for personvern følges opp i egen resultatenhet. Det vises deretter til *Oppdragsbeskrivelse for resultatenhetsledere* knyttet til informasjonssikkerhet.[61] I denne fremgår det blant annet at resultatenhetslederne har følgende ansvar:

- Enheten skal jevnlig dokumentere en systematisk vurdering av om uvedkommende får tilgang til informasjon som følge av enhetens informasjonsbehandling
- Enheten skal rapportere og følge opp avvik … som fører til at interne eller eksterne uvedkommende får tilgang til informasjon
- Enheten skal ha en dokumentert plan eller tiltakskort i «CIM» for å håndtere situasjoner som følge av at informasjon blir tilgjengelig for interne eller eksterne vedkommende

Det fremgår ikke, og er heller ikke lagt inn lenke, i oppdragsbeskrivelsen knyttet til overordnete rutiner for arbeidet med å hindre uautorisert innsyn i konfidensielle opplysninger for resultatenhetsledere.

I *Oppdragsbeskrivelse for akseptabel bruk av IKT*[62] som gjelder for alle ansatte i Bergen kommune fremgår kommunens krav til ansatte når det gjelder informasjonsforvaltning og taushetsplikt, brukerkonto, systemtilganger, passord og PIN, bruk av kommunens IKT-systemer og –utstyr og innsyn og overvåkning.

[61] Oppdrag – personvern og informasjonssikkerhet for resultatenhetsledere. Ikke datert
[62] Oppdrag for alle ansatte for akseptabel bruk av IKT. Ikke datert

Oppdragsbeskrivelsen skal signeres elektronisk før det blir gitt tilgang i kommunens IKT-utstyr og -systemer, og ansatte må årlig re-kvittere for at å ha lest og forstått innholdet. Revisjonen får opplyst at det ikke er egne regler i skolesektoren knyttet til konfidensialitet utenom den allmenne plikten som følger av *Akseptabel bruk av IKT*.

I dokumentet fremgår blant annet følgende regler for å hindre uautorisert innsyn i konfidensielle opplysninger:

- Det er ikke tillatt å søke etter, lese eller på annen måte tilegne seg, bruke eller besitte opplysninger uten at det er begrunnet i tjenstlig behov.
- Datamaskinen skal låses når den forlates i løpet av arbeidstiden. Datamaskinen låser seg automatisk først etter 20 minutter.
- Informasjon som er taushetsbelagt, intern, sensitiv eller som på annen måte stiller krav til lagring, arkivering og informasjonssikkerhet, skal ikke lagres utenfor Bergen kommunes systemer, uten at det foreligger en databehandleravtale.

På *Allmenningen*[63] er det videre lagt inn informasjon om bruk av passord og PIN-koder, blant annet knyttet til hvordan et sikkert passord bør utformes, håndtering av passord og relevante utdrag fra *Reglement for akseptabel bruk av IKT* som gjelder passord og PIN-koder. Det er videre lagt inn lenke til *passordhjelpen*[64] og kommunens overordnede passordinstruks.[65] I passordinstruksen får de ansatte tips til hvordan å lage et sikkert passord samt en gjennomgang av den enkelte medarbeiders plikt til å behandle passord etter kommunens reglement.[66]

Kommunen opplyser at det fra og med 22. mars 2019 ble aktivert to-faktorautentisering på alle system i skolen hvor det lagres for eksempel elevnavn, skoletilhørighet og klassetilhørighet.[67] Revisjonen får videre opplyst at kommunen på revisjonstidspunktet var i gang med å innføre nytt oppvekstadministrativt system (Vigilo) for alle de kommunale skolene i Bergen. Vigilo har to-faktorautentisering.

Systemkoordinatorene forteller at de har vært sentrale i arbeidet med å få på plass to-faktorautentisering i systemene som benyttes i skolene, og at det gikk en melding ut til alle skolene ved årsskiftet 2018/2019 at de hadde tre uker på å få på plass metode for to-faktorautentisering (SMS, kodeark, Microsoft Authenticator e.l.). Deretter låste man nesten alle system til to-faktorautentisering gjennom eFeide i februar 2019.

I intervju blir det fortalt at for alle de store programmene som er tilgjengelig for alle brukere må man logge seg på via eFeide. Det blir lagt til at det per i dag[68] bare er itslearning hvor man logger seg på via to-faktorautentisering utenfor eFeide.

Selv om kommunen har låst de fleste system til to-faktorautentisering gjennom eFeide, er det fortsatt mulig å logge inn på flere av dem utenom denne løsningen med en standard pålogging med brukernavn og passord. Systemkoordinatorene forteller at de har kontaktet leverandører for å få lukket dette sikkerhetshullet.

Revisjonen får opplyst at det er sårbarheter knyttet til uautorisert innsyn i familierelasjoner i flere av systemene som er i bruk i skolesektoren. Dette gjelder for eksempel i det nye sak-/arkivsystemet BK360. Etter det revisjonen får opplyst, er det i dette systemet mulig for alle saksbehandlere i kommunen å finne familierelasjoner for enhver person i kommunen. For eksempel kan en saksbehandler som behandler en søknad om bygging av garasje eventuelt se hvilke barn denne søkeren har.

---

[63] Se https://allmenningen.bergen.kommune.no/ansatthjelpen/informasjonstjenester-og-ikt/systemer-tilganger-og-passord
[64] Tjeneste for å nullstille og få tilsendt midlertidig passord til PC/intern sone.
[65] Overordnet passordinstruks. Revisjonsdato: 13.06.2018. Gyldig til 31.05.2019.
[66] Når det gjelder bruk av passord forteller systemkoordinatorene at passordene til ansattes PC-er må endres jevnlig. Dersom en bruker er inaktiv vil passordet utgå etter to måneder.
[67] Fellesadministrasjonen i BBSI sendte den 22. mars 2019 ut et fellesskriv adressert til alle skolene i kommunen hvor det blir informert om at to-faktorautentisering skal innføres. Det fremgår i skrivet at BBSI allerede på det daværende tidspunkt har innført to-faktorautentisering på systemene itslearning, eFeide, Conexus Engage og klassetrivsel.no. *Aktivering av tofaktor for ansatte i skolene.* BBSI – Fellesadministrasjonen, Dato: 22. mars 2019.
[68] Intervjureferatet ble verifisert 3. oktober 2019.

Som tidligere nevnt, kom det mot slutten av revisjonsperioden frem opplysninger om at det var avdekket brudd på informasjonssikkerheten knyttet til uautorisert innsyn i konfidensielle opplysninger i Vigilo (se også *Rutiner for risikovurderinger av informasjonssikkerhet* i avsnitt 3.3.7). Da Vigilo ble tatt i bruk høsten 2019, ble det oppdaget at det hadde blitt sendt meldinger fra noen skoler til foresatte som står registrert som foreldre til barnet i det sentrale folkeregisteret, også dem uten foreldreansvar.[69] Disse meldingene inneholdt informasjon om Vigilo, navnet på skolen til barnet, og lenke til informasjonsskriv fra de respektive skolene. Kommunen understreker at disse e-postene og informasjonsskrivene ikke inneholdt konfidensiell informasjon. Innlogging i Vigilo gav tilgang til barnets navn, skole, klasse, navn på ansatte ved barnets skole, samt navn på andre foresatte knyttet til barnet.

Kommunen opplyser at ingen foresatte uten foreldreansvar til barn med skjermet adresse fikk slik melding eller har logget seg på Vigilo. Kommunen opplyser imidlertid at det er ukjent hvor mange av de 477 foresatte uten foreldreansvar til barn som ikke bor på skjermet adresse som fikk e-posten gjennom Vigilo som leste denne. Kommunen opplyser at 107 av dem logget seg på systemet.

Kommunen sentralt mottok melding om informasjonssikkerhetsbruddet 3. september.[70] 4. september satte kommunen stab og orienterte Datatilsynet muntlig om hendelsen. 5. september ba kommunen leverandøren av Vigilo om å fjerne alle relasjoner mellom barn og foresatte uten foreldreansvar i systemet, for slik å sikre at disse ikke lenger hadde mulighet til å logge seg på systemet. 6. september ble Kripos varslet av kommunen.

Til tross for at kommunen opplyser at alle relasjoner mellom barn og foresatte uten foreldreansvar skulle bli fjernet i Vigilo tidlig i september, kom det i oktober frem opplysninger om at ikke alle slike relasjoner var fjernet. Ved minst én skole stod fortsatt en foresatt uten foreldreansvar på mottakerlisten i Vigilo da det ble sendt ut e-post fra Vigilo med påloggingsinformasjon til systemet.[71] I forbindelse med verifiseringen av rapporten opplyser kommunen at sletting av foresatte uten foreldreansvar ble bestilt og bekreftet slettet fra leverandør, men at leverandør i ettertid har bekreftet at denne jobben sannsynligvis ikke var komplett.

Kommunen meldte avvik til Datatilsynet 2. oktober. Informasjonssikkerhetsbruddet ble holdt unntatt offentlighet for å sikre at kommunen fikk gitt de involverte tilstrekkelig oppfølging.[72]

Revisjonen har mottatt opplysninger og dokumentasjon på at kommunen både har satt i verk og planlegger å sette i verk tiltak for å redusere risikoen for uautorisert innsyn i systemet.[73] Tiltakene er knyttet direkte til fagsystemet og det aktuelle informasjonssikkerhetsbruddet.

Etterlevelse i skolesektoren

Revisjon får i intervju opplyst at det før innføringen av BK360 var en konfidensialitetsproblemstilling knyttet til at alle elevmapper var i papirform og at man fikk utdelt hele elevmappen til en elev uavhengig av behov for innsyn og informasjon. På denne måten fikk ansatte ved utdeling av elevmapper ofte innsyn i mer enn det som var tjenstlig nødvendig (mer om elevmapper og BK360 under avsnitt 4.4.1).

Rektorene som deltok i spørreundersøkelsen fikk spørsmål om skolen har etablert praksis når det gjelder å hindre uautorisert innsyn i konfidensielle opplysninger. 89 % av rektorene svarer «ja» på dette spørsmålet, mens 5 % svarer «nei» og 7 % svarer «vet ikke». Rektorene fikk videre spørsmål om å vurdere grad av risiko for at uautoriserte personer får innsyn i konfidensielle opplysninger på skolen. Svarene er gjengitt i figur 15:

---

[69] Vigilo hadde vært operativt siden 12. mai 2019, men uten at informasjon om at systemet var i drift eller hvordan man skulle logge seg på og benytte seg av det var distribuert.

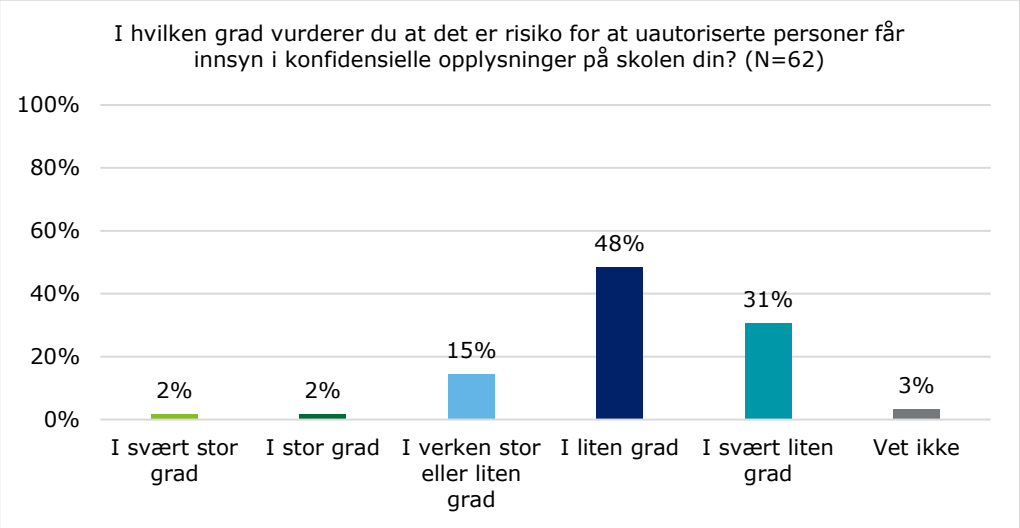
[70] Seks dager før informasjonssikkerhetsbruddet ble registrert i kommunen (28. august), ble leverandøren av Vigilo varslet av en forelder om at foresatte uten foreldreansvar automatisk var lagt inn i systemet. Dagen etter varslet vedkommende forelder politiet og rektor ved den aktuelle skolen. Se avsnitt *Rutine for håndtering av avvik* på side 29.

[71] Oppslag i Bergens Tidende 25. oktober 2019: https://www.bt.no/nyheter/lokalt/i/4qGM2e/kommunen-lovet-at-alle-uten-foreldreansvar-var-ute-av-skoleappen-saa-f

[72] Se https://www.bergen.kommune.no/omkommunen/avdelinger/byradsavd-for-barnehage-skole-og-idrett/346/article-163127 og *Svar på krav om tilsvar etter melding om avvik i Vigilo* 11. november 2019.

[73] Avviksmelding fra Bergen kommune til Datatilsynet (datert 2. oktober 2019), samt *Prosedyrebeskrivelse for innlesing av persondata i Vigilo* (dater 15. oktober 2019).

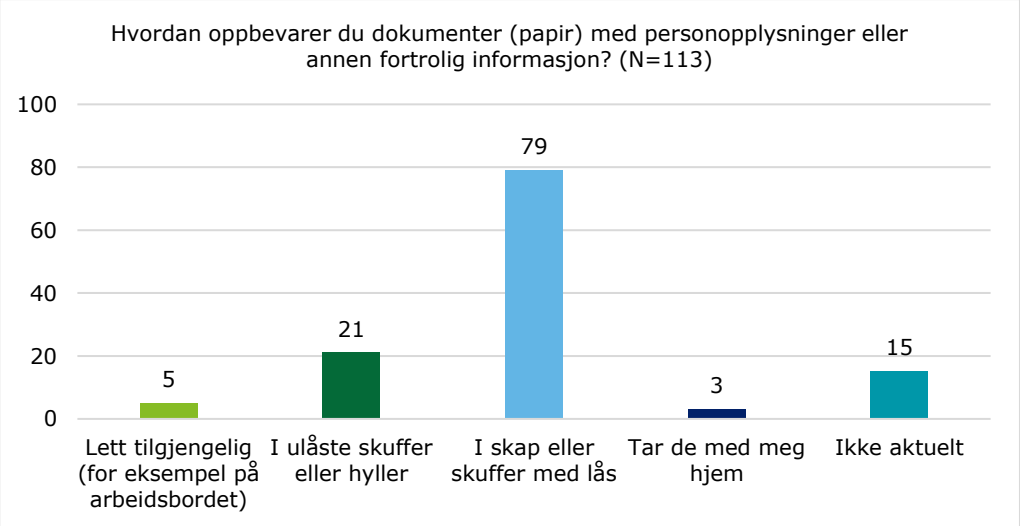
Figur 15: Risiko for brudd på konfidensialitet



Som vist i figur 15, svarer totalt 79 % at det «i liten grad» (48 %) eller «i svært liten grad» (31 %) er risiko for at uautoriserte personer får innsyn i konfidensielle opplysninger på skolen, mens totalt 4 % svarer at det er «i svært stor grad» (2 %) eller «i stor grad» (2 %) risiko for dette.

Medarbeiderne i skolesektoren som deltok spørreundersøkelsen[74] fikk spørsmål knyttet til informasjons-sikkerhetspraksis i arbeidshverdagen. I figur 16 fremgår svarene fra respondentene om oppbevaring av dokumenter med personopplysninger eller annen fortrolig informasjon:

Figur 16: Oppbevaring av konfidensielle dokumenter[75]



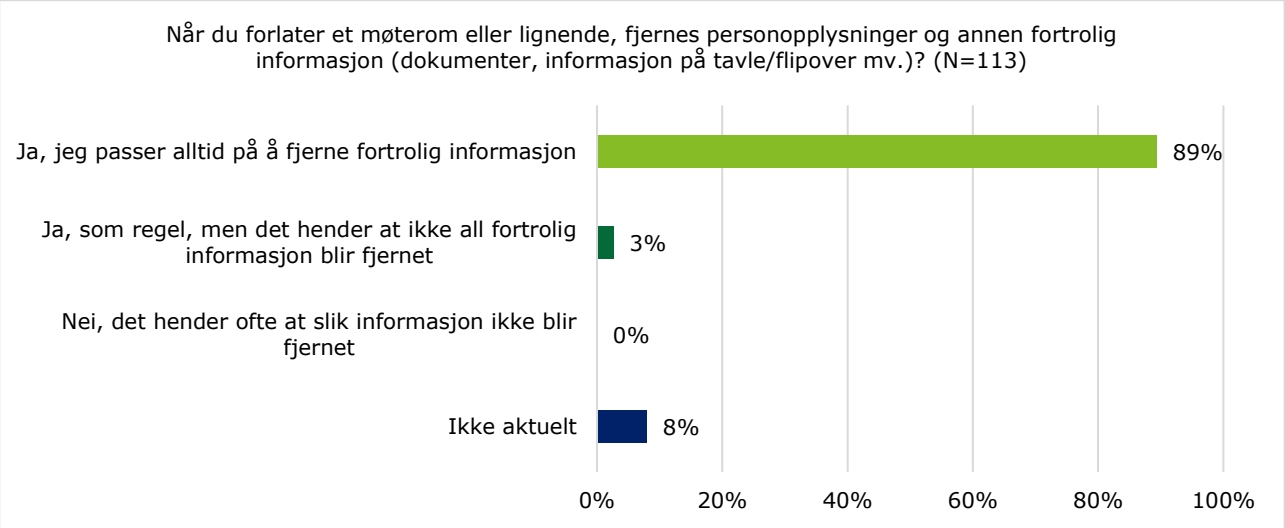
På spørsmål om praksis ved utskrift av dokumenter som inneholder konfidensiell informasjon svarer 46 % at de alltid henter utskriften med en gang, mens over 40 % oppgir at de benytter styrt utskrift.[76]

[74] Dette spørsmålet ble stilt til respondentene som oppgir at de behandler eller kommer i kontakt med personopplysninger, sensitive personopplysninger og/eller annen fortrolig informasjon i sin arbeidshverdag.
[75] Respondentene kunne svare flere alternativ og resultatene er derfor ikke prosentuert.
[76] Også kalt «follow me» eller «sikker utskrift». Rundt 5 % svarer at de bruker skriver på eget kontor. Ingen av respondentene velger alternativet «det hender at jeg lar utskriften ligge for å hente den når jeg går forbi», og om lag 6 % oppgir at dette ikke er aktuelt for dem

110 av 113 respondenter svarer at de makulerer papirene når de skal kaste dokumentasjon som inneholder personopplysninger eller annen fortrolig informasjon, mens to svarer at de kaster disse papirene i «vanlig papirinnsamling eller i bosset».[77]

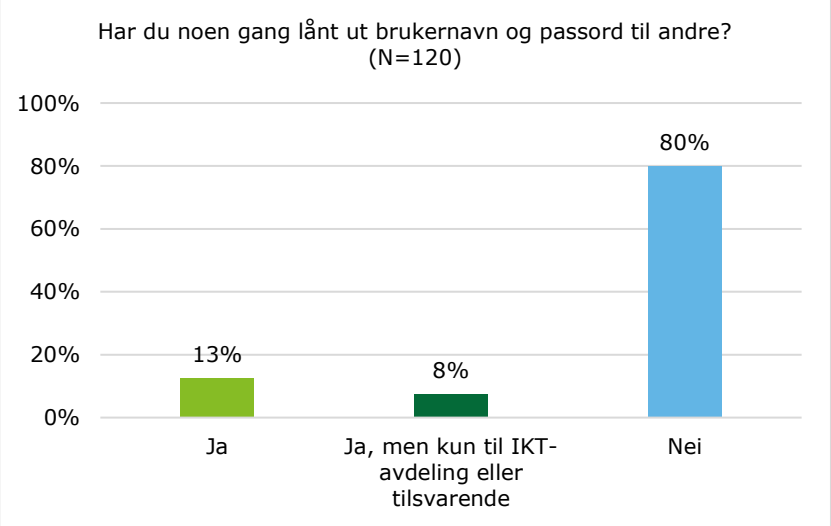
På spørsmål om praksis når man forlater møterom fordeler svarene seg som vist i figuren under:

Figur 17: Praksis når man forlater møterom e.l.



I spørreundersøkelsen til ansatte ble det stilt spørsmål om praksis når det gjelder utlån av brukernavn og passord. Som vist i figur 18, svarer om lag 80 % «nei» på spørsmålet om de noen gang har lånt ut brukernavn og passord til andre, mens rundt 13 % svarer «ja», og ca. 8 % av respondentene svarer «ja, men kun til IKT-avdeling eller tilsvarende».

Figur 18: Utlån av brukernavn og passord



Videre ble respondentene bedt om å svare på hva de vanligvis gjør når de i løpet av arbeidsdagen forlater PC-en de bruker.[78] 3 % av respondentene svarer «ingenting, tenker ikke så mye på det», 17 % svarer «baserer meg på at datamaskinen låses automatisk» og 11 % «lukker ned åpne vinduer med informasjon om personopplysninger». Over 40 % svarer at de «logger ut og/eller slår av datamaskinen», mens 27 % «låser datamaskinen ved hjelp av tastatur eller låseknapp».[79]

[77] Den siste respondenten svarer «ikke aktuelt» på dette spørsmålet.
[78] N=120
[79] 1 % svarer «ikke aktuelt».

4.3.2 Vurdering

Gjennom styringssystemet for personvern og informasjonssikkerhet med tilhørende dokumenter, har Bergen kommune formalisert ansvar og oppgaver knyttet til å hindre uautorisert innsyn i konfidensielle opplysninger. Særlig relevant er oppdragsbeskrivelsene som inngår i styringssystemet, der ansvaret til resultatenhetslederne for å hindre uautorisert innsyn i konfidensielle opplysninger går frem, og der reglene som skal etterleves av de ansatte for å hindre uautorisert innsyn i konfidensielle opplysninger er nedfelt.

Revisjonen vil understreke at informasjonssikkerhetsbruddet knyttet til innsyn i konfidensielle opplysninger i forbindelse med implementeringen av Vigilo, tyder på at verken system, rutiner eller ansvars- og oppgaveforhold for å hindre uautorisert innsyn i konfidensielle opplysninger er tilstrekkelig ivaretatt i skolesektoren i Bergen kommune.

Som informasjonssikkerhetsbruddet knyttet til Vigilo videre illustrerer, har det vært og er det fortsatt sårbarheter knyttet til risiko for uautorisert innsyn i konfidensielle opplysninger; basert på det revisjonen har fått opplyst, er det iverksatt tiltak for å utbedre noen av disse. Revisjonen vil i den forbindelse peke på at flere av tiltakene vi er gjort kjent med knytter seg til det nevnte informasjonssikkerhetsbruddet, og ikke nødvendigvis til de bakenforliggende årsakene som forårsaket at informasjonssikkerhetsbruddet fant sted. For å redusere sannsynligheten for at sårbarheter blir utnyttet eller at informasjonssikkerhetsbrudd skjer, må de bakenforliggende årsaken til risikoene identifiseres på systemnivå, og treffende tiltak settes i verk, for eksempel knyttet til etterlevelse av kommunens system og rutiner, samt med hensyn til tydeliggjøring av oppgaver og ansvar (se også seksjon 3.4).

Revisjonen registrerer ellers at kommunen våren 2019 aktiverte to-faktorautentisering for alle systemer i skolen hvor det lagres visse typer opplysninger om elever. Dette er et teknisk tiltak som bidrar til å hindre uautorisert innsyn i konfidensielle opplysninger. Revisjonen merker seg imidlertid at det fortsatt var mulig å omgå slik to-faktorautentisering i flere av systemene som er i bruk i skolesektoren. Revisjonen er oppmerksom på at det er pågående prosesser for å utbedre slike sikkerhetshull, men på revisjons-tidspunktet var ikke disse ferdigstilte.

Når det gjelder skolenes praksis for å hindre uautorisert innsyn i konfidensielle opplysninger i skole-sektoren, svarer rektorene i spørreundersøkelsen at de i overveiende grad har en etablert praksis knyttet til dette, og videre at de gjennomgående vurderer risikoen for brudd på konfidensialitet på skolene som lav. Sett i sammenheng med svarene i spørreundersøkelsen til de ansatte i skolesektoren når det gjelder etterlevelse av rutiner for å hindre uautorisert innsyn i konfidensielle opplysninger, er det grunn til å stille spørsmål ved rektorenes svar og vurderinger; blant de ansatte i skolesektoren svarer 21 % av respondentene at de enten har delt passordet sitt med IT-avdelingen eller andre. Det å dele passord med andre er ikke i samsvar med grunnleggende prinsipp for informasjonssikkerhet, heller ikke dersom det er IT-avdelingen man deler passordet med, og utgjør en stor risiko for konfidensialitetsbrudd.

Undersøkelsen viser videre at det både forekommer at dokumenter med personopplysninger eller annen fortrolig informasjon blir oppbevart i ulåste skuffer eller hyller, at de denne typen papirdokument oppbevares lett tilgjengelig, og at ansatte tar med seg konfidensielle papirdokument hjem. Også slik praksis utgjør vesentlig risiko for brudd på konfidensialiteten.

4.4 Lagring av konfidensielle opplysninger i sikker sone

4.4.1 Datagrunnlag

Retningslinjer og rutiner

Som del av kommunens styringssystem for personvern og informasjonssikkerhet er det, som nevnt under avsnitt 4.3.1, utarbeidet en oppdragsbeskrivelse for alle ansatte for *Akseptabel bruk av IKT*[80] som skal gjennomgås og kvitteres av alle ansatte før de får tilgang til kommunens IKT-systemer. I dokumentet blir det under overskriften *Informasjonsforvaltning og taushetsplikt* blant annet vist til at:

- Alle skal være bevisst hvilken type informasjon de behandler, og hvilke krav som stilles til sikring av informasjonen.

[80] Oppdrag for alle ansatte for akseptabel bruk av IKT. Ikke datert.

- Informasjon skal alltid arkiveres i kommunens sak- og arkivsystem eller fagsystem. Først når informasjon er arkivert kan man vurdere å slette eller makulere kopier, utskrifter o.l.[81]

På *Allmenningen* er det videre tilgjengeliggjort en rutine for klassifisering av informasjon.[82] Formålet med denne er å «legge til rette for at all informasjon i Bergen kommune er tilstrekkelig sikret i henhold til hvilke krav som stilles til informasjonssikkerhet etter norsk lov». Rutinen beskriver at informasjon i kommunen skal klassifiseres i én av tre kategorier/soner; *sikker*, *intern* eller *åpen.* De tre kategoriene og tilhørende sikringskrav er nærmere omtalt i rutinen, og informasjon som lagres i skolen er nevnt som eksempler både for kategorien *sikker* og *intern*. Rutine for klassifisering av informasjon er ikke tilgjengelig på sidene som omhandler informasjonssikkerhet og personvern på *Allmenningen*. I intervju med systemkoordinatorer hos BBSI kommer det frem at de ikke kjenner til rutinen. I forbindelse med verifiseringen av rapporten peker kommunen på at rutinen for klassifisering av informasjon er brukt som mal i ROS-analysene, og at klassifisering av behandlet personopplysninger er dokumentert.

Revisjonen får opplyst at skolene inntil nylig ikke har hatt digitale arkivsystem, men har arkivert konfidensielle opplysninger som for eksempel elevmapper i fysiske arkivskap. Kommunen er nå i prosess med å innføre nytt sak-/arkivsystem (BK360) i skolen, der man blant annet kan lagre elevmapper og informasjon om ansatte elektronisk. Kommunen opplyser at i tillegg til åpenbare gevinster ved digitalisering av oppgaver, er den viktigste årsaken til innføring av BK360 å gjøre saksbehandling og arkivering sikkert. Kommunen opplyser videre at grensesnittet i det nye saksbehandlingssystemet også reduserer sannsynligheten for å gjøre saksbehandlingsfeil med personopplysninger.

På *Allmenningen* finner man informasjon om BK360 gjennom *Ansatthjelpen* og siden *Saksbehandling og arkiv.* Blant annet foreligger det her informasjon om *Arkiver for oppvekst* hvor det er lagt inn oversikt over hvordan dokumenthåndteringen for skoler skal utføres og hva som er arbeidsdelingen mellom enhetene og Bergen byarkiv.[83]

Kommunen informere at det som ledd i prosessen med å innføre nytt saks-/arkivsystem skal gjennomføres opplæring i å lagre personsensitive opplysninger for elever og ansatte i henholdsvis elev- og personal-mapper i alle enhetene.

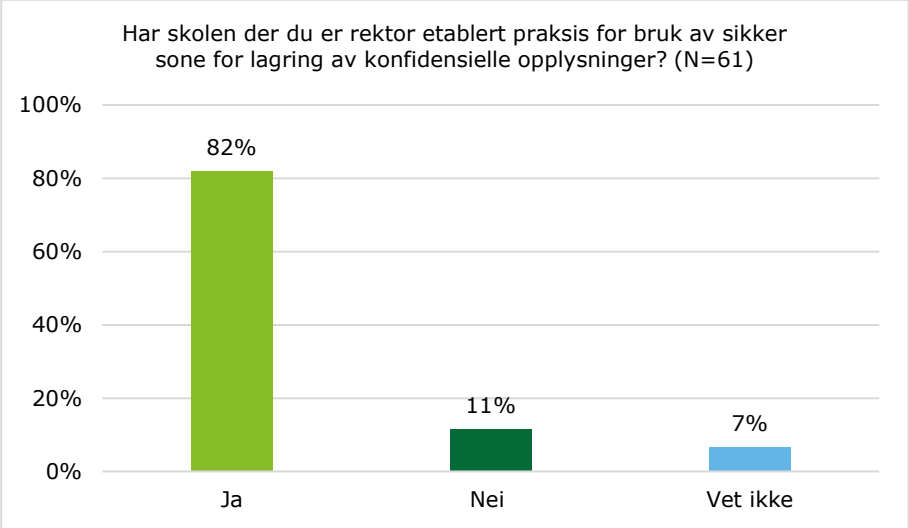
Det blir opplyst at BK360 ble implementert våren 2019 og at det er seksjon for digitalisering og innovasjon konsern (SDI) i byrådsavdeling for finans, innovasjon og eiendom (BFIE) som er systemansvarlig for sak- og arkivsystemet. Avvikling av manuelle mapper i tradisjonelle arkivskap er en pågående prosess i skolene som følge av innføringen av BK360. Det blir fortalt i intervju at nåværende rutine er at alle elevmapper skal legges inn på sikker sone i det nye sak- og arkivsystemet, men at ikke alle elevmapper som foreligger i papirform vil skannes.

Etterlevelse i skolesektoren

Rektorene som deltok i spørreundersøkelsen fikk spørsmål om det er etablert praksis for å bruke sikker sone for lagring av konfidensiell informasjon ved skolen:

[81] Det går videre frem under dette punktet at man i tilfeller der man er i tvil skal kontakt nærmeste leder eller Bergen Byarkiv.
[82] Rutine for klassifisering av informasjon. Målgrupper: leder, system- og tjenesteeier og medarbeider/ansatt. Godkjent av leder for informasjonssikkerhet. Datert 23.10.2017, gyldig til 31.12.2019.
[83] Siden *Brukerveiledning: hvordan opprette elevsak og -dokument* går det frem at man alltid skal bruke tilgangskoden *UO Elev- Unntatt offentlighet* når man oppretter en ny elevsak, og at man må velge skolens tilgangsgruppe eller *INGEN Elev.* Skolens tilgangsgruppe gir tilgang til alle ansatte på skolen og arkivansvarlige (Sentralarkivet). Tilgangsgruppe INGEN Elev gir tilgang til den som oppretter saken, administrasjonen på skolen og arkivansvarlige. På *Allmenningen* er det også lagt inn rutiner gjeldende for elever og barnehagebarn på hemmelig adresse. Et av punktene her er at man skal vurdere om det skal settes egen tilgangsgruppe på eleven/barnet.

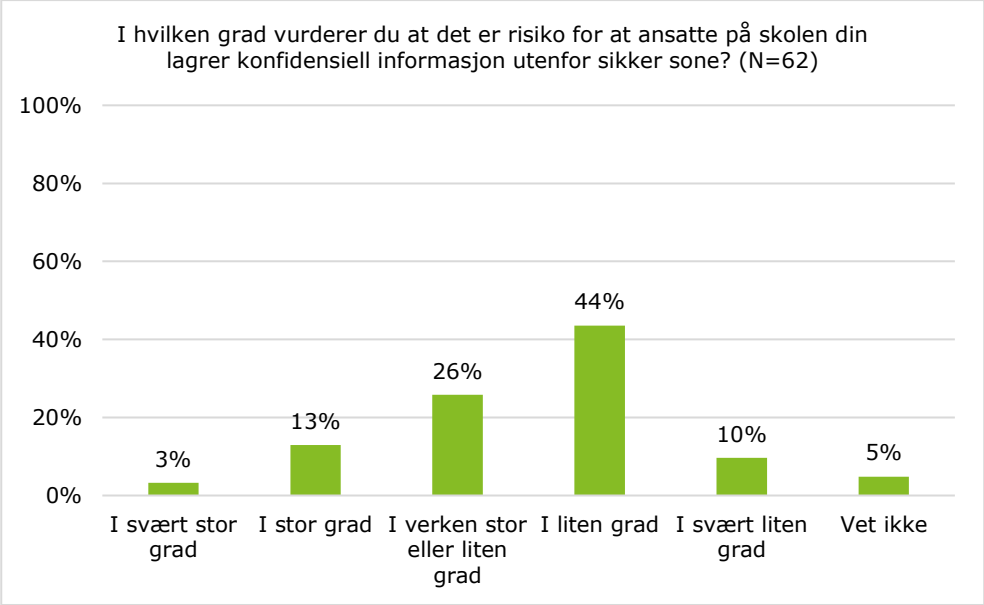
Figur 19: Praksis for lagring av konfidensielle opplysninger



11 % svarer at det ikke er etablert praksis for å bruke sikker sone for lagring av konfidensielle opplysninger, og 7 % av respondentene svarer «vet ikke».

På spørsmål til rektorene om hvorvidt de vurderer at det er risiko for at ansatte på skolen lagrer konfidensiell informasjon utenfor sikker sone fordeler svarene seg som vist i figur 20:

Figur 20: Risiko for lagring av konfidensiell informasjon utenfor sikker sone



16 % av rektorene svarer at det vurderer at det «i svært stor grad» eller «i stor grad» er risiko for at ansatte lagrer konfidensielle opplysninger utenfor sikker sone. 5 % svarer «vet ikke» på dette spørsmålet, mens 26 % vurderer at det «i verken stor eller liten grad» er risiko for dette.

4.4.2 Vurdering

Bergen kommune har noen rutiner og retningslinjer for lagring av konfidensielle opplysninger. I tillegg til reglene som fremgår i *Akseptabel bruk av IKT*, har kommunen retningslinjer for klassifisering av informasjon og tilhørende prosedyrer for hvor ulik type informasjon skal lagres.

Retningslinjene for klassifisering av informasjon ser ikke ut til å være en integrert del av i kommunens styringssystem for personvern og informasjonssikkerhet. Dette kan være en medvirkende årsak til at retningslinjene ikke var kjent for dem som ble intervjuet. Det vurderes uansett som uheldig at det som

eksisterer av utfyllende retningslinjer knyttet til sikker lagring av konfidensielle opplysninger verken er kjent eller inngår i styringssystemet for informasjonssikkerhet, da dette gir økt sannsynlighet for feil og slik risiko for at konfidensiell informasjon lagres uten tilstrekkelig sikring.

Undersøkelsen viser ellers at skolesektoren er i prosess med å ta i bruk kommunens nye sak-/arkivsystem (BK360). Gitt at skolesektoren frem til dette har hatt papirbaserte arkiver for elevmapper o.l., innebærer overgangen til BK360 en klar forbedring med hensyn til sikker lagring av konfidensielle opplysninger. Revisjonen merker seg videre at det både foreligger veiledningsmateriell for dokumenthåndtering i BK360 for skolesektoren, og at det som ledd i implementering av systemet er planlagt opplæring i lagring av sensitiv informasjon for ansatte.

Når det gjelder skolenes praksis for lagring av konfidensielle opplysninger, svarer rektorene i spørre-undersøkelsen at de i overveiende grad har en etablert praksis knyttet til dette. Revisjonen registrerer videre at litt over halvparten av rektorene vurderer risikoen for at konfidensiell informasjon lagres utenfor sikker sone som lav, men òg at en relativt stor del av dem (16 %) vurderer denne risikoen som høy.

I sum er det revisjonens vurdering at det i skolesektoren bare delvis er etablert rutiner og praksis for sikring av konfidensialitet med hensyn til bruk av sikker sone for lagring av konfidensielle opplysninger.

4.5 Kryptering av konfidensielle opplysninger

4.5.1 Datagrunnlag

Retningslinjer og rutiner

Kommunens styringssystem for personvern og informasjonssikkerhet setter krav til kryptering gjennom oppdragsbeskrivelser og retningslinjer. I *Oppdragsbeskrivelsen for alle ansatte for akseptabel bruk av IKT* blir det stilt krav om at:

- IKT-utstyr som benyttes til behandling av gradert, beskyttelsesverdig eller taushetsbelagt informasjon skal være kryptert
- Ansatte skal sørge for at mobiltelefon, minnepenn, minnekort er beskyttet (kryptert), der dette er gjennomførbart
- Taushetsbelagt eller sensitiv informasjon skal ikke sendes per e-post, med mindre disse opplysningene er kryptert.

Oppdragsbeskrivelse for systemeiere er del av styringssystemet for personvern og informasjonssikkerhet i Bergen kommune. Det blir der vist til at systemeiere må sørge for at IKT-systemet eller IKT-løsningen ivaretar nødvendige sikringstiltak, og at vedkommende videre blant annet skal ha oversikt over om systemet er sikret i henhold til *Sjekkliste for grunnsikring av IKT-systemer i Bergen kommune.*[84]

Revisjonen har fått tilgang til den ovenfornevnte sjekklisten.[85] Den er delt inn i to: 1) systemtekniske grunnkrav og 2) driftsmessige grunnkrav med tilhørende beskrivelser av tiltak. Under systemtekniske grunnkrav er det en tiltakskategori om kryptering med følgende «mulige tiltak til vurdering»:

- Alle data bør være kryptert ved lagring
- Krypteringen bør være basert på en unik krypteringsnøkkel per kunde
- Krypteringsnøkler bør være beskyttet mot uautorisert tilgang og tap

På *Allmenningen* er det en beskrivelse av hvordan å beskytte innhold i e-poster. Her står det at det i kommunen ikke er tillat å sende taushetsbelagt informasjon, sensitiv informasjon eller «særlige kategorier av personopplysninger» på e-post uten å kryptere informasjonen. Videre er det lagt inn en beskrivelse av hvordan man kan bruke Office-pakkens krypteringsfunksjon for å beskytte innholdet i e-poster. Det er ikke forklart, eller lagt ved lenke til forklaring av, hva som inngår under taushetsbelagt informasjon, sensitiv informasjon eller «særlige kategorier av personopplysninger».

Kommunen opplyser at de nylig har innført *Vigilo* som oppvekstadministrative systemet (se mer om dette under avsnitt 4.3.1). Systemet har en kommunikasjonsmodul med hovedformål å sørge for at dag til dag-

[84] Det er ikke lagt inn lenke eller forklaring i dokumentet om hvor man finner den nevnte sjekklisten.
[85] Sjekkliste for grunnsikring av IKT-systemer. Revisjonsdato 14.05.2019. Gyldig til 13.09.2019. Det fremgår av dokumentet at sjekklisten blant annet er inspirert av SINTEFs anbefalinger i «Cloud Security Requireents v. 2.0»

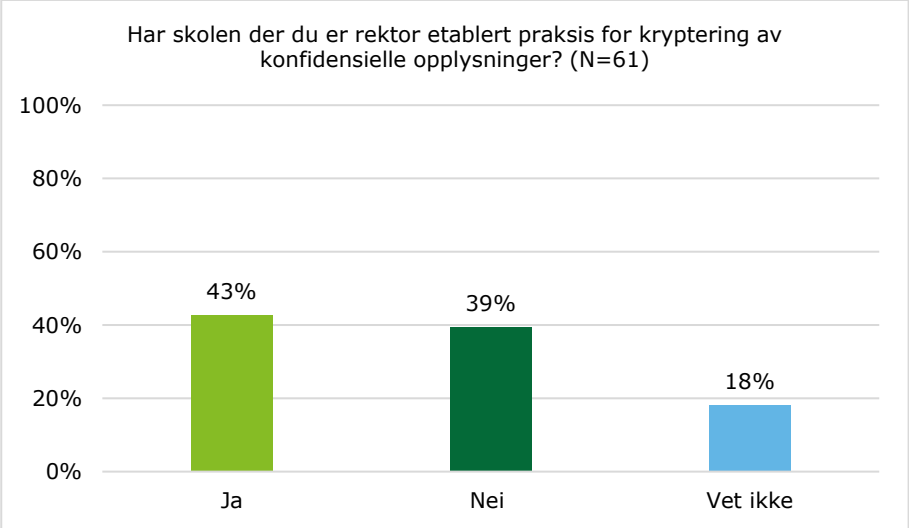
kommunikasjon mellom skole/barnehage og hjem blir gjort på en trygg og effektiv måte. Kommunikasjonsmodulen er et alternativ til e-post, ranselpost og telefonsamtaler, og vurderes av kommunen som egnet til å gi bedre oversikt og sikre effektiv og trygg informasjonsflyt mellom skole/barnehage og hjem. Løsningen er kryptert og sannsynligheten for feilsendinger oppgis av kommunen å være liten.[86]

Kommunen opplyser videre at resultatenhetene er instruert, blant annet gjennom områdemøter, om at personopplysninger aldri skal sendes i e-post.

Etterlevelse i skolesektoren

I spørreundersøkelsen som gikk ut til rektorene i Bergen kommune ble det stilt spørsmål om skolen der vedkommende er resultatenhetsleder har etablert praksis for kryptering av konfidensielle opplysninger. Svarene er gjengitt i figur 21:

Figur 21: Praksis for kryptering av konfidensielle opplysninger

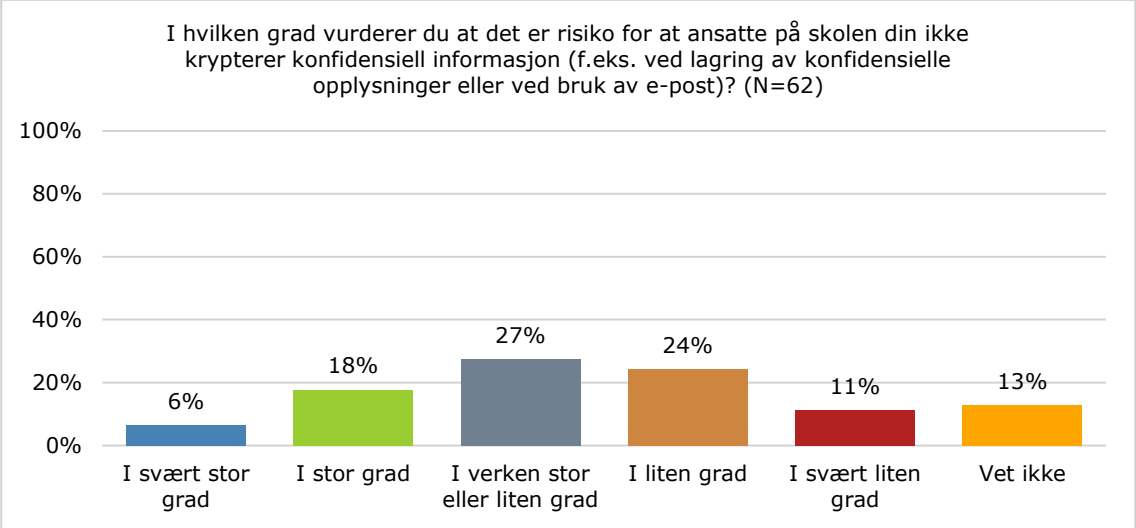


Som vist i figuren, svarer litt flere «ja» (43 %) på spørsmålet, enn som svarer «nei» (39 %). Nesten én av fem (18 %) svarer «vet ikke».

Rektorene ble videre bedt om å vurdere risikoen for at ansatte på skolen ikke krypterer konfidensiell informasjon. Svarene er gjengitt i figur 22:

[86] Kommunen understreker i forbindelse med verifiseringen av rapporten at *Vigilo* innføres som nytt oppvekstadministrativt system i Bergen kommune, og at dette omfatter søknad og opptak i barnehage, SFO, fakturering, redusert betaling, administrasjon av elever, timeplaner, fravær, karakterer og rapportering. En liten del av løsningen er kommunikasjonsmodulen mellom skole, barnehage og hjem. Videre opplyser kommunen at da Vigilo la ut ny funksjonalitet i denne kommunikasjonsmodulen – som hverken var bestilt eller godkjent av Bergen kommune – valgte kommunen 25. oktober å inntil videre stenge kommunikasjonsmodulen. Kommunen understreker at øvrige funksjoner i Vigilo er i drift. Det var denne nye funksjonaliteten som er omtalt i media: https://www.bt.no/nyheter/lokalt/i/Op05vb/bergen-kommune-stenger-deler-av-skoleappen-vigilo.

Figur 22: Risiko knyttet til kryptering



Som det fremgår av figuren, svarer til sammen 24 % at det «i svært stor grad» eller «i stor grad» er risiko for dette, mens totalt 35 % svarer at det «i liten grad» eller «i svært liten grad» er slik risiko.[87]

4.5.2 Vurdering

Bergen kommune har gjennom prosedyrer, rutiner og retningslinjer tilgjengeliggjort på *Allmenningen* stilt krav til kryptering av konfidensielle opplysninger. Både i oppdragsbeskrivelser, sjekklister og mer detaljert veiledningsmateriell går det frem hvilke typer opplysninger og informasjon som krypteres. Det går også tydelig frem at for eksempel ulike kategorier av sensitive opplysninger / konfidensiell informasjon ikke skal sendes ukryptert per e-post.

Revisjonen merker seg videre at skolesektoren relativt nylig innførte et fagsystem som blant annet skal brukes i korrespondanse mellom kommunen og foresatte til barn i skolen. Korrespondansen i fagsystemet er kryptert, og sikrer slik at personopplysning og sensitive personopplysninger ikke sendes ukryptert.

Svarene til rektorene i spørreundersøkelsen indikerer at skolene bare delvis har en praksis for å kryptere konfidensielle opplysninger. Nesten én av fem av dem vet ikke om skolen har praksis for dette, mens bare litt flere svarer at skolen har etablert praksis for dette enn dem som svarer at de ikke har det. Også vurderingen av risikoen for at ansatte på skolene ikke kryptere konfidensiell informasjon tyder på at dette kan være en utfordring i skolesektoren; nesten én av fire av rektorene vurdere denne risikoen som høy.

I sum er det revisjonens vurdering at det sentralt i kommunen er etablert rutiner for sikring av konfidensialitet gjennom kryptering av konfidensielle opplysninger. Funn i undersøkelsen tyder imidlertid på at skolesektoren i praksis bare delvis følger disse.

[87] 27 % svarer «i verken stor eller liten grad», mens 13 % svarer «vet ikke».

5. Tilgangsstyring

5.1 Problemstilling

I dette kapittelet vil vi svare på følgende problemstilling med underproblemstillinger:

Har skolesektoren etablert rutiner for tilgangsstyring, og etterleves disse?

Under dette:

a) Hindring av uautorisert tilgang til informasjonssystemene
b) Inn- og utmelding av ansatte i relevante informasjonssystemene
c) Vurdering av om ansatte har riktige tilganger i informasjonssystemene
d) Loggføring av brukte tilganger i informasjonssystemene

5.2 Revisjonskriterier

Personvernforordningen artikkel 32 nr. 1 stiller krav om informasjonssikkerhet ved behandling av personopplysninger. Kravene som blir stilt er at man skal sette i verk egnede tekniske og organisatoriske tiltak basert på risikovurderinger for å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene. Tiltak som også blir nevnt under artikkel 32 nr.1 er pseudonymisering og kryptering av personopplysninger og evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse.

Se vedlegg 3 for utfyllende revisjonskriterier.

5.3 Hindring av uautorisert tilgang til informasjonssystemene

5.3.1 Datagrunnlag

Retningslinjer og rutiner

Det er leder av EDD som er ansvarlig for den tekniske ivaretakelsen av sikkerheten i kommunens IKT-infrastruktur, mens den enkelte systemeier skal sørge for at deres system oppfyller kravene til informasjonssikkerhet som nedfelt i *Reglement for trygg digitalisering*. Begge disse ansvarsområdene innbefatter også å hindre uautorisert tilgang til informasjonssystemene.

Alle ansatte i Bergen kommune må kvittere for at de har lest og akseptert *Oppdragsbeskrivelse for akseptabel bruk av IKT* før de får tilgang til kommunens informasjonssystemer, og de må re-kvittere årlig for å beholde sine tilganger. Utover dette er ikke regler, rutiner eller retningslinjer for tilgangsstyring eller hindring av uautorisert tilgang til informasjonssystemer nærmere omtalt i kommunens sentrale styrende dokumenter for informasjonssikkerhet.

På *Allmenningen* er det imidlertid tilgjengeliggjort regler og rutiner for tilgangsstyring; gjennom lenken *Ansatthjelpen*, *Informasjonstjenester og IKT* og deretter *Systemer*, *tilganger og passord* er det flere menypunkt som omhandler tilganger til kommunens informasjonssystemer. Sentralt blant disse er siden *Bestille, endre og slette brukerid/*brukertilgang. System og rutiner for tilgangsstyring og etterlevelse av disse kan bidra til å hindre uautorisert tilgang til informasjonssystemene. Dette er nærmere omtalt i avsnitt 5.4.1.

Videre har kommunen regler, rutiner og instrukser knyttet til passordutforming og passordbruk (se avsnitt 4.3.1), og som nevnt i samme avsnitt, er det som ledd i å sikre konfidensialitet også innført to-faktor-autentisering på de fleste fellessystem i skolene. Både regler for passordutforming og -bruk, og to-faktor-autentisering er relevante organisatoriske og tekniske tiltak for å hindre uautorisert tilgang til informasjons-systemer.

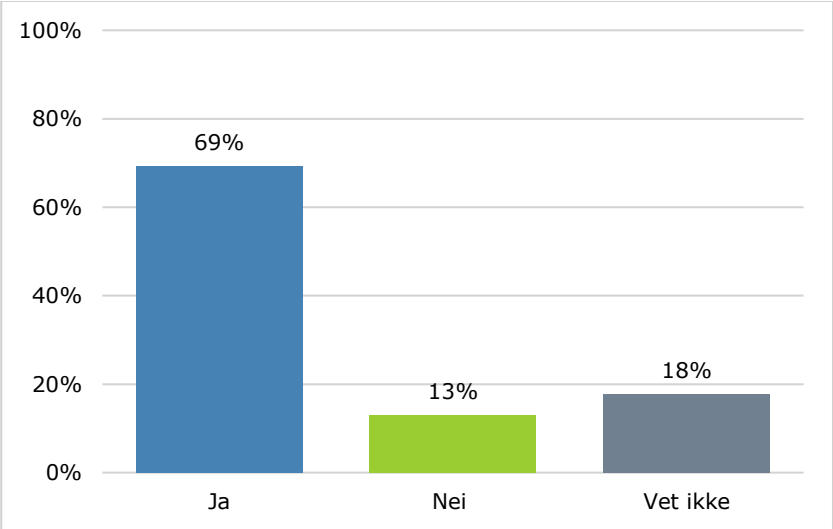
Etterlevelse i skolesektoren

I intervju med systemkoordinatorene blir det fortalt at tilgangsstyringen fungerer bra i de store systemene der byrådsavdelingen er systemeier, som for eksempel Extens;[88] her er systemkoordinatorene trygge på at ingen ansatte har tilganger som de ikke skal ha. I de mindre systemene er det imidlertid risiko for at tilgangsstyringen ikke er like god, da systemkoordinatorene er mer fokusert på pedagogikken i og bruken av systemet heller enn brukertilgang og kontrollen på denne. Det blir nevnt at det er risiko for at brukere kan ha brukertilganger de ikke har tjenstlig behov for i disse mindre systemene; dette gjelder for eksempel system for nasjonale prøver.

Når det gjelder BK360 forteller systemkoordinatorene at dette systemet styres sentralt og er innenfor EDDs ansvarsområde.

Rektorene som deltok i spørreundersøkelsen ble stilt spørsmål om skolen har «etablert praksis knyttet til å hindre uautorisert tilgang til informasjonssystemene» som benyttes.[89] Svarene er gjengitt i figur 23:

Figur 23: Praksis for å hindre uautorisert tilgang til informasjonssystemene

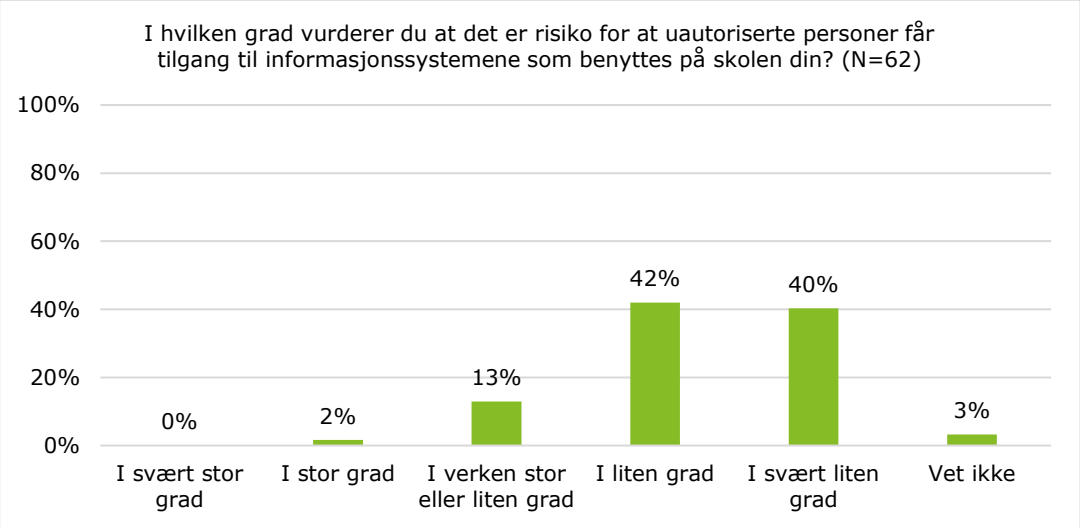


Videre fikk rektorene spørsmål om i hvilken grad de vurderer at det er risiko for at uautoriserte personer får tilgang til informasjonssystemene på skolen. Svarene er gjengitt i figur 24:

[88] Extens er master for ca. 80 integrerte system, som for eksempel Conexus Engage (kartleggingsverktøy). Tilgangsstyringen til alle de integrerte systemene går via Extens. I Extens registreres elever og blant annet deres tilhørighet til klasser og lærere, samt karakterer og fravær. Ved endt skolegang er det dette systemet man henter vitnemål fra.

[89] N=62

Figur 24: Risiko for uautorisert tilgang til informasjonssystemene



Som vist i figur 24, svarer totalt 82 % av rektorene at de vurderer denne risikoen som «liten» eller «svært liten», mens 2 % vurderer at det «i stor grad» er risiko for dette.[90]

Teknisk etterlevelse

Revisjonen har gjennomført tekniske undersøkelser av kommunens IKT-systemer for å avdekke og teste eventuelle identifiserte sårbarheter som muliggjør uautorisert tilgang til informasjonssystemene.

Den ene sikkerhetstesten hadde som primærfokus å avdekke hvorvidt eksisterende sikkerhetskontroller og/eller filtreringsmekanismer (primært brannmurer) forhindrer uautorisert tilgang til tjenester og tilgrensende nettverk. Testen ble gjennomført via fjerntilgang til tre fysiske maskiner som stod i kommunens interne nettverk. Én av disse var konfigurert som en regulær PC for ansatte, én som en elev-PC, og én var uten restriksjoner. Gjennom de tildelte testbrukerne kunne revisjonen simulerer situasjoner hvor bruker med tilsvarende rettigheter som testbrukerne er kompromittert eller forsøkes utnyttes av eksisterende bruker.

Sikkerhetsvurderingen ble gjennomført i form av en penetrasjonstest hvor det ble gjort flere tjeneste- og sårbarhetsskanninger med formål om å kartlegge eksponerte tjenere og tjenester, og eventuelle sårbarheter i de identifiserte tjenester. Videre ble det gjort forsøk på ulike tilnærminger for å omgå eksisterende sikkerhetsmekanismer. Sikkerhetstesten ble gjennomført delvis manuelt, og delvis ved bruk av ulik spesialisert programvare.[91]

Funn og sårbarheter identifisert i testen ble kategorisert etter risiko (tabell 8).

Tabell 8: Risikovurdering

Konsekvens				
	Høy	Moderat	Høy	Kritisk
	Moderat	Lav	Moderat	Høy
	Lav	Lav	Lav	Moderat
		Lav	Medium	Høy
		Sannsynlighet		

Risikoen er beregnet ut ifra estimert *sannsynlighet* og *konsekvens* (tabell 9).

[90] 0 % svarte «i stor grad», 13 % svarte «i verken stor eller liten grad» og 3 % svarte «vet ikke».
[91] For nærmere tekniske beskrivelser av testene vises det til vedlegg 6.

Tabell 9: Rangering av sårbarheter etter sannsynlighet og konsekvens

	Sannsynlighet	Konsekvens
Høy	Sårbarheter som lett lar seg avdekke og som enkelt lar seg utnytte av en angriper. Disse sårbarhetene er tilgjengelig for et stort antall angripere. En angriper trenger bare avgrenset teknisk kompetanse og ressurser for å kunne utnytte slike sårbarheter.	Sårbarheter som gjør det mulig for en angriper å manipulere sensitiv informasjon, skade Bergen kommunes omdømme, tilrane seg uautorisert tilgang til sensitiv informasjon, IKT-tjenester og/eller infrastruktur. Denne typen sårbarheter kan gjøre det mulig for en angriper å tilrane seg privilegerte tilganger, inkludert tilgang til andre systemer i Bergen kommune.
Moderat	Utnyttelse av disse sårbarhetene er mer sofistikert. Sårbarhetene kan bare utnyttes av et begrenset antall angripere, de er ikke lette å oppdage og/eller en angriper trenger teknisk kompetanse og/eller tilgang på mye ressurser for å kunne utnytte sårbarhetene.	Sårbarheter som gjør det mulig for en angriper å skade Bergen kommunes omdømme eller tilrane seg uautorisert tilgang til informasjon. Privilegiene en angriper kan tilrane seg ved å utnytte disse sårbarhetene er noe begrenset.
Lav	Sårbarhetene kan ikke utnyttes enkelt. Disse sårbarhetene er vanskelige å oppdage, de er bare tilgjengelige for et lavt antall angripere, og/eller de krever avansert teknisk kompetanse og/eller tilgang på sofistikerte ressurser for å utnyttes.	Sårbarheter som i seg selv ikke utgjør noen fare, men som kan føre til tap av informasjon knyttet til kommunens nettverk, og som en angriper kan nyttiggjøre seg av videre. Utnyttelse av disse sårbarhetene gir en angriper helt begrensete privilegier i systemet.

Det ble ikke avdekket sårbarheter med kritisk risiko. Det ble blant annet ikke avdekket sårbarheter som gjorde det mulig å eskalere privilegiene på elevkontoen slik at denne fikk tilgang til ansattressurser. Det ble imidlertid avdekket én sårbarhet med høy risiko, og fire med moderat risiko. For eksempel ble det identifisert sårbarheter som kan muliggjøre at en elevkonto får tilgang til en annen elev-PC.

Revisjonen gjennomførte også en sikkerhetstest av fagsystemet *itslearning*. Formålet med denne testen var å vurdere fagsystemets sikkerhetsmekanismer for å forhindre uautorisert tilgang til brukerdata og administrativ funksjonalitet. Det ble gjort tekniske undersøkelser av autentiserings- og autoriserings-mekanismene i fagsystemet, med særlig fokus på mulige feil og mangler i disse. Videre ble det gjort tekniske tester av den underliggende infrastrukturen for å undersøke om denne inneholdt feil-konfigurasjoner eller kjente sårbarheter.

Gjennomgangen av autentiserings- og autoriseringsmekanismene ble fra brukergruppene «elev», «lærer» og «administrator». Det ble gjort kontrollerte forsøk på å eskalere privilegiene fra hver brukergruppe for å undersøke om det var mulig å få uautoriserte tilganger i andre brukergrupper. I tillegg ble det gjort kontrollerte forsøk på å få uautorisert tilgang til brukerdata innen hver brukergruppe.

Funn og sårbarheter identifisert i testen ble kategorisert etter risiko (tabell 8).

Tabell 10: Risikovurdering

Konsekvens				
	Høy	Moderat	Høy	Høy
	Moderat	Lav	Moderat	Høy
	Lav	Lav	Lav	Moderat
		Lav	Medium	Høy
		Sannsynlighet		

Risikoen er beregnet ut ifra estimert *sannsynlighet* og *konsekvens* (tabell 11):

Tabell 11: Rangering av sårbarheter etter sannsynlighet og konsekvens

	Sannsynlighet	Konsekvens
Høy	Når konfigurasjonssårbarheter eller sårbarheter finnes som er umiddelbart mulige å utnytte, eller når sårbarheter finnes som tidligere har forårsaket sikkerhetshendelser i systemet.	Tap av konfidensialitet, integritet eller tilgjengelighet av kritisk data, systemer eller infrastrukturkomponenter, som forårsaker nedetid, eksponering av kritiske data eller uautorisert modifisering av kritiske data.
Moderat	Når mulige eller faktiske sårbarheter finnes der særlige forutsetninger må være tilstede for at disse kan utnyttes, eller når det mangler eller er svakheter i operasjonelle prosedyrer.	Tap av konfidensialitet, integritet eller tilgjengelighet av data, systemer eller infrastrukturkomponenter som ikke er kritiske, men som forårsaker betydelige utfordringer for brukere eller tjenestemottagere, eller som påvirker systemet negativt.
Lav	Når det er mindre tekniske utfordringer i oppsettet eller feilkonfigurasjoner som ikke er umiddelbart mulig å utnytte, og/eller når det er mindre mangler i operasjonelle prosedyrer e.l.	Tap av konfidensialitet, integritet eller tilgjengelighet av data, systemer eller infrastrukturkomponenter som ikke er kritiske, og som kun forårsaker mindre utfordringer for brukere eller tjenestemottagere, eller som i mindre grad påvirker systemet negativt.

Sikkerhetstesten avdekket ingen sårbarheter med høy risiko. Det ble imidlertid avdekket tre sårbarheter kategorisert med moderat risiko, og åtte kategorisert med lav risiko.[92]

5.3.2 Vurdering

Ansvaret og de overordne oppgavene for å hindre uautorisert tilgang til informasjonssystemene er gjennom kommunens styringssystem for personvern og informasjonssikkerhet delt mellom EDD og systemeiere. Videre er det i *Oppdragsbeskrivelse for akseptabel bruk av IKT* nedfelt noen overordnede rutiner for å hindre uautorisert tilgang til informasjonssystemene. Også de generelle rutinene knyttet til tilgangsstyring (se seksjon 5.4), regler, rutiner og instrukser knyttet til passordutforming og passordbruk (se seksjon 4.3), samt innføringen av to-faktorautentisering (også seksjon 4.3), bidrar alle til å hindre uautorisert tilgang til informasjonssystemene i kommunen.

Funn i undersøkelsen tyder på at det i de større systemene eid av skolesektoren er relativt lav risiko for at uautoriserte får tilgang, mens risikoen for dette vurderes som høyere for de mindre, pedagogiske systemene som benyttes.

Svarene til rektorene i spørreundersøkelsen indikerer at skolene i relativt stor grad har en praksis som hindrer uautorisert tilgang til informasjonssystemene, og de vurderer også gjennomgående risikoen for at uautoriserte får tilgang til informasjonssystemene som i overveiende grad lav.

I sikkerhetstesten som fokuserte på de tekniske foranstaltningene for å forhindre uautorisert tilgang til tjenester og tilgrensende nettverk, ble det ikke avdekket kritiske sårbarheter. Det ble imidlertid identifisert sårbarheter med både høy, moderat og lav risiko.

I sikkerhetstesten av fagsystemet *itslearning* ble det ikke avdekket sårbarheter med høy risiko, men det ble avdekket sårbarheter med både moderat og lav risiko.

Funnene fra sikkerhetstestene viser at det er viss risiko for at det kan oppstå brudd på informasjonssikkerheten med hensyn til uautorisert tilgang til informasjonssystemene i skolesektoren. Revisjonen mener det må iverksette tiltak for å redusere disse mulighetene. For tekniske detaljer knyttet til dette, viser revisjonen til funn og vurderinger i vedlegg 6 og vedlegg 7.

[92] Se vedlegg 7 for detaljer.

5.4 Inn- og utmelding av ansatte i informasjonssystemene

5.4.1 Datagrunnlag

Rutiner og retningslinjer

Det fremgår gjennom *Oppdrag - informasjonssikkerhet og personvern for resultatenhetsledere* i kommunens styringssystem for informasjonssikkerhet og personvern at skolene skal «føre en dokumentert oversikt over hvilken informasjon den behandler, hvor og av hvem».

Som nevnt i avsnitt 5.3, er det på *Allmeningen* tilgjengelig informasjon om hvordan å *bestille, endre og slette brukerid/brukertilgang*.[93] Her beskrives fremgangsmåten for å opprette ny bruker og endre på eksisterende bruker for ulike byrådsavdelinger. Det fremgår at bestilling av brukerkonto for nyansatte gjøres via et eget nettverktøy (Bestillingsweb). Gjennom dette verktøyet får brukere tilgang til standardprogrammer (e-post, skriveprogram, og regneark), og det velges hvilke fellesområder brukeren skal ha tilgang til.

Det er nærmeste leder som skal bestille tilganger til ansatte gjennom Bestillingsweb. Kommunen oppgir at risikoen for at ansatte får tildelt tilganger de ikke skal ha ved ansettelse er lav, selv om det kan skje at ikke alle tilgangene er på plass fra dag én.

Det går ellers frem hva som er ansattes ansvar ved skifte av arbeidssted i kommunen, og tilsvarende hva som er både gammel og ny leders ansvar. Den ansatte som skifter arbeidssted i kommunen må selv melde fra til nåværende leder om at man skal endre arbeidssted slik at brukerid/e-post ikke blir slettet.

I tilfellene der en arbeidstaker skifter arbeidssted i kommunen går det frem på *Allmenningen* at det er enklest at ny leder «henter» bruker og bestiller tilganger til fellesområder og systemer i henhold til de oppgavene ansatt skal ha på den nye arbeidsplassen. Endringer registreres via Bestillingsweb. «Avtroppende» leder må bestille fjerning av tilganger som bruker ikke lenger skal ha.

Det blir påpekt at det er viktig med god kommunikasjon mellom ny leder, forhenværende leder og ansatt i denne prosessen.

På samme intranettsiden er det lagt inn lenke til *Retningslinje for håndtering av inaktive kontoer*, som beskriver hvordan brukerkontoer og personlige data (e-post, hjemmeområde o.l.) skal håndteres når kontoen ikke blir brukt i lengre. Det blir presisert at sletting av konto, med tilhørende e-postkasse og hjemmeområde, kun skal gjøres når dette er bestilt av nærmeste leder, eventuelt overordnet leder, eller avdeling for personvern og informasjonssikkerhet (personvernombudet).

Det er på samme siden på *Allmenningen* informasjon til ledere om deaktivering av tilganger når en ansatt tar permisjon eller slutter. Her er det også lagt inn lenke til en annen intranettside med overskrift *Ansatt slutter – sjekkliste innen IKT;* en sjekkliste som skal benyttes av leder når en ansatt avslutter sitt arbeidsforhold i kommunen.[94] I sjekklisten fremgår det at det er resultatenhetsledere som har ansvar for at alle systemtilganger oppheves når en ansatt slutter. Melding om avsluttet tilgang skal primært skje via systemet *Bestilingsweb*, men også systemeier/systemkoordinator skal ha melding når ansatte slutter.

Det fremgår videre i sjekklisten at resultatenhetsleder skal påse at brukerfullmakter og brukertilganger i fagsystem avbestilles/deaktiveres. Tilganger som for eksempel skal avsluttes i systemet eFeide skal meldes til systemkoordinator, mens avslutting av tilganger til blant annet det sentrale folkeregisteret skal meldes til EDD via Helpdesk.

Etterlevelse i skolesektoren

Revisjonen får opplyst at de fleste systemene i kommunen går gjennom *single sign-on*, noe som betyr at når en brukerkonto er deaktivert i det sentrale systemet (av EDD), får ikke vedkommende logget på datamaskinen sin, og mister dermed også tilgang til informasjonssystemene.

---

[93] På *Allmenningen* blir det informert at ansatte i kommunen som arbeider i skole, barnehage, idrett eller bibliotek har en egen lisensavtale og er derfor definert som en egen brukertype.

[94] Det fremgår i sjekklisten at man finner informasjon om tema på *bestille, endre og slette brukerid* på Bergen kommunes intranettsider.

Det fremgår videre at det er risiko for at tilganger ikke avsluttes dersom ansatte endrer stilling innad i kommunen. Brukerkontoer blir automatisk flyttet i det sentrale systemet når en ansatt endrer stilling, men ikke alle tilganger følger automatisk i denne prosessen. Det understrekes at det er systemeiere som skal følge opp at ansatte ikke har unødvendige tilganger til systemet.

Systemkoordinatorene forteller at det er rektor sitt ansvar å sluttmelde brukere som ikke lenger skal ha tilgang til system, men at dette ikke alltid blir utført. Systemkoordinatorene mener at det er stort forbedringspotensial knyttet til system for sluttmelding av brukere, og opplever at rektorene syns det er utfordrende at det ikke er en samlet ordning for å melde behov for tilgang til nye ansatte.

Det fremgår videre i intervju at det er risiko for at det kan gå lang tid før tilganger blir slettet dersom en ansatt skifter arbeidsplass innenfor BBSI eller er langvarig sykemeldt. Det er systemkoordinatorene som skal sørge for at ansatte mister tilganger, men de er avhengig av dialog med den enkelte leder for å få informasjon om tilganger som skal slettes.

I intervju med systemkoordinatorene blir det fortalt at i Extens har ansatte bare tilgang til tildelte elevgrupper på skolen man er ansatt på. Dersom ansatte skifter arbeidssted må de be rektor om ny tilgang i Extens, hvorpå vedkommende må kontakte systemkoordinator og be om dette.

Systemkoordinator for Extens forteller videre at det er etablert praksis at hun ved skolestart hvert år sender en liste med brukere i systemet til rektorene og ber dem bekrefte at det er de registrerte brukerne som skal ha tilgang til systemet. Ved tilbakemelding fra rektorene sletter systemkoordinator tilganger og melder eventuelt nye brukere på kurs for deretter å gi disse tilgang i systemet. Revisjonen har fått tilsendt en huskeliste for bruk ved nytt skoleår, der blant annet «lage brukerliste og sende til skoler» er ført opp som et punkt når det gjelder Extens-systemet. Det fremgår ikke hvor eller om huskelisten er tilgjengeliggjort for medarbeidere med ansvar som systemeiere eller systemkoordinatorer.

I spørreundersøkelsen til rektorene i bergensskolene ble det stilt spørsmål om skolene har etablert praksis for inn- og utmelding av ansatte i informasjonssystem.[95] 94 % av rektorene svarer «ja» på dette spørsmålet mens 3 % av rektorene svarer henholdsvis «nei» og «vet ikke».

5.4.2 Vurdering

Bergen kommune har system og rutiner for tilgangsstyring. Undersøkelsen viser at ikke alle tilganger følger automatisk når en ansatt skifter arbeidssted innad i kommunen, og videre at det er forbedringspotensial knyttet til selve prosessen med å sikre riktige tilganger (se også seksjon 5.3). Revisjonen mener derfor at kommunens system og rutiner for tilgangsstyring bare i noen grad er egnet til sikre at ansatte får tilgangene de trenger når de trenger dem, og for å sikre at ansatte som slutter i kommunen mister tilgangene sine.

Revisjonen merker seg at det i intervju blir påpekt at det er systemeiere som har ansvar for å sikre at ansatte i skolene har rette tilganger, og at det er rektorene som skal melde fra om hvem som trenger hvilke tilganger. Sett i sammenheng med funnene i kapittel 3 knyttet til uklarheter og usikkerhet ved både systemeieres og resultatenhetslederes rolle og ansvar med hensyn til informasjonssikkerhet i skole-sektoren, er det etter revisjonens vurdering en viss sannsynlighet for at tilganger ikke opprettes i tide, og en noe større sannsynlighet for at tilganger ikke stenges ned ved bytte av arbeidsplass internt i kommunen eller avslutning av arbeidsforhold i kommunen. Det er følgelig risiko for at ansatte ikke har tilganger de trenger, og en noe større risiko for at ansatte i kommunen har tilganger de ikke har tjenstlig behov for.

Revisjonen registrerer ellers at ikke alle rektorer er bevisst sitt ansvar når det gjelder sluttmelding av brukere, og vurderer at dette ytterligere øker risikoen for at ansatte har tilganger de ikke har tjenstlig behov for. Det fremgår av undersøkelsen at det potensielt kan gå lang tid før tilganger slettes ved langvarig fravær eller skifte av arbeidssted internt i kommunen.

[95] N=62

5.5 Vurdering av riktige tilganger i informasjonssystemene

5.5.1 Datagrunnlag

Retningslinjer og rutiner

Det fremgår i *Oppdrag – personvern og informasjonssikkerhet for resultatenhetsledere* at enheten skal føre en dokumentert oversikt over *hvilken* informasjon den behandler, *hvor* og av *hvem*.

Som nevnt i avsnittene over er det lagt inn retningslinjer på *Allmenningen* for inn- og utmelding av ansatte i kommunens informasjonssystem, samt rutiner for hva som skal gjøres ved endring av arbeidssted innad i kommunen. Det fremgår at både ansatt, nærmeste leder og eventuelt ny leder (ved bytte av arbeidssted innad i kommunen) har ansvar knyttet til oppretting og avslutting av tilganger.

Revisjonen har ikke mottatt opplysninger om at det på sentralt nivå i kommunen eller i skolesektoren er etablert rutine eller praksis for å gjøre systematiske vurderinger av om ansatte har riktige tilganger.

Etterlevelse i skolesektoren

Som nevnt i avsnitt 5.4.1 får revisjonen opplyst at det er risiko for at tilganger ikke avsluttes dersom ansatte endrer stilling innad i kommunen, og at det er systemeiere som skal følge opp at ansatte ikke har unødvendige tilganger til systemet.

Kommunen opplyser at vurdering av riktige tilganger i skolesektoren styres gjennom rettigheter i det enkelte system og at det er systemkoordinator for de enkelte systemene som oppretter tilganger. Som eksempel blir det vist til at behov for tilgang til Oppvekstadministrativt system (OA-system) blir meldt fra rektorer og styrere til systemkoordinator.

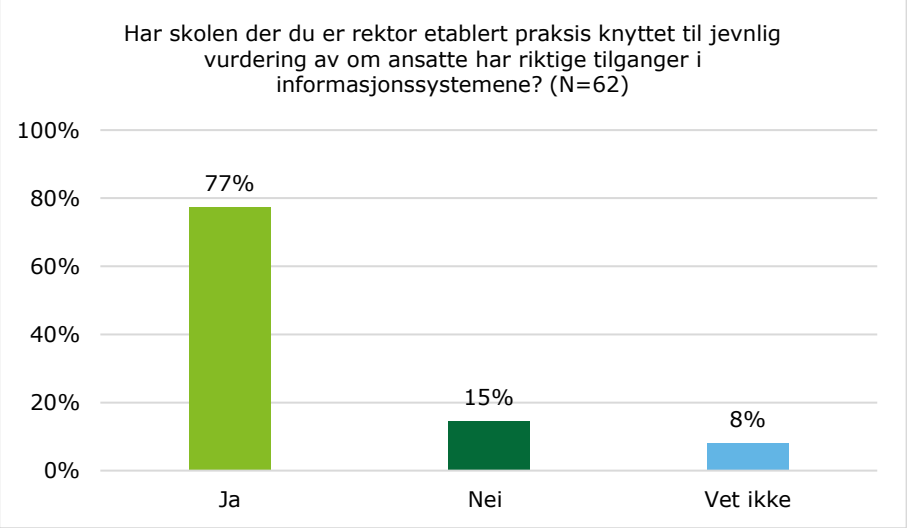
Det fremgår videre at behov for tilgang til en del system må meldes via IKT-koordinator som er autorisert bestiller. IKT-koordinator må da kontrollere at vedkommende har et tjenstlig behov for tilgang før dette bestilles. I noen tilfeller så må IKT-koordinator dokumentere dette behovet videre til SDI før tilgang gis.

IKT-koordinator forteller at han opplever at systemkoordinatorene stort sett har oversikt over tilganger i systemene, da tilgang til informasjonssystem blir styrt av jobbrollen til den ansatte.

Som nevnt i avsnitt 5.4.1 har systemkoordinator for Extens en årlig rutine der hun sender en liste over ansatte med tilgang til rektorene og ber de trekke fra og legge til hvilke ansatte på skolen som skal ha tilgang i systemet. Dette er et eget punkt i huskelisten *Nytt skoleår – huskelister systemer.* Andre punkt i huskelisten er «rydde rektorer i PAS og Vokal», «slette/endre bruker gamle elever i itslearning». Det fremgår ikke hvor eller om huskelisten er tilgjengeliggjort.

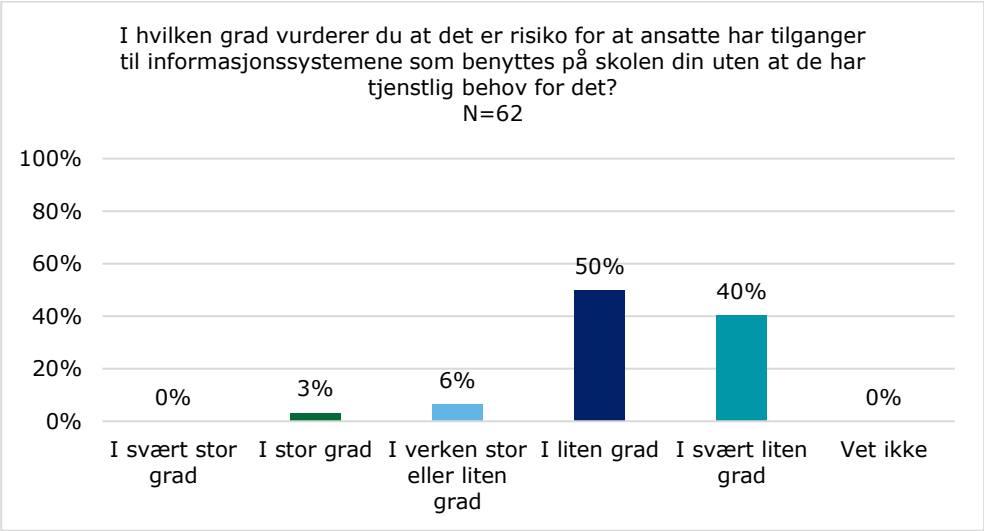
Rektorene som deltok i spørreundersøkelsen fikk spørsmål om det er etablert praksis knyttet til jevnlig vurdering av om ansatte har riktige tilganger i informasjonssystemene. Som vist i figur 25 svarer 15 % «nei» og 8 % «vet ikke» på dette spørsmålet:

Figur 25: Vurdering av tilganger



Videre fikk rektorene gjennom spørreundersøkelsen i oppgave å vurdere i hvilken grad det er risiko for at ansatte har tilganger til informasjonssystemene uten at de har tjenstlig behov for dette:

Figur 26: Risiko for unødvendige tilganger



Som fremstilt i figur 26 vurderer 3 % av rektorene som deltok i spørreundersøkelsen at det «i stor grad» er risiko for at ansatte har tilganger uten tjenstlig behov for dette, mens 6 % vurderer at det «i verken stor eller liten grad» er risiko for dette. De aller fleste (totalt 90%) vurderer at det «i liten grad» (50 %) eller «i svært liten grad» (40 %) er risiko for dette ved deres skoler.

Rektorene ble også bedt om å vurdere risikoen for at «ansatte ikke har tilganger til informasjonssystemene som benyttes på skolen din, men som de har tjenstlig behov for». [96] På dette svarer 8 % at det «i stor grad» er risiko for dette, mens rundt 18 % vurderer at det «i verken stor eller liten grad» er risiko for dette. 3 % oppgir at de ikke vet hvorvidt dette er en risiko.[97]

5.5.2 Vurdering

Undersøkelsen viser at Bergen kommune har system og rutiner for tilgangsstyring. Som nevnt i vurderingen i avsnitt 5.4.2, mener revisjonen at disse rutinene bare i noen grad er egnet til sikre at ansatte i kommunen får tilgangene de trenger og mister tilgangene de ikke har tjenstlig behov for.

Undersøkelsen viser at mye av ansvaret knyttet til tilgangsstyring ligger hos rektorene og systemeiere/systemkoordinatorer. Med henvisning til funn i kapittel 3 knyttet til resultatenhetsledere og systemeieres delvis manglende oppfyllelse av eget informasjonssikkerhetsansvar, mener revisjonen det er risiko for at ansatte i skolesektoren har tilganger de ikke skulle hatt, og videre at det bør iverksettes tiltak for å redusere denne risikoen.

Sett i sammenheng med det som kommer frem i avsnitt 5.4.1, vurderer revisjonen at praksisen for å vurdere riktige tilganger er sårbar. Undersøkelsen viser at sikringen av riktige tilganger avhenger av flere roller, og det fremgår for eksempel at rektor ikke alltid sluttmelder brukere. Videre vurderes praksis med årlige justering av tilganger som sårbar. Revisjonen vil påpeke at skriftliggjøring av rutiner er en viktig del av tydeliggjøringen av roller og ansvar innenfor et område, og kan bidra til å sikre at tjenester og tilbud er mindre sårbart ved permisjon, sykdom eller annet fravær.

Undersøkelsen viser videre at praksis knyttet til vurdering av riktige tilganger ikke er tilstrekkelig innarbeidet i organisasjonen; nesten én av fire rektorer som deltok i spørreundersøkelsen svarer at det ikke er eller at de ikke vet om det er praksis knyttet til jevnlig vurdering av riktige tilganger. Revisjonen mener dette ikke er tilfredsstillende all den tid det er rektorene som er ansvarlige for å melde videre behovet for endringer i tilgangene til informasjonssystemene.

[96] N=62
[97] 45 % svarer «i liten grad» og 26 % svarer «i svært liten grad».

5.6 Loggføring av brukte tilganger i informasjonssystemene

5.6.1 Datagrunnlag

Som nevnt fremgår det i *Oppdrag – personvern og informasjonssikkerhet for resultatenhetsledere* at enheten skal føre en dokumentert oversikt over hvilken informasjon den behandler, hvor og *av hvem.*

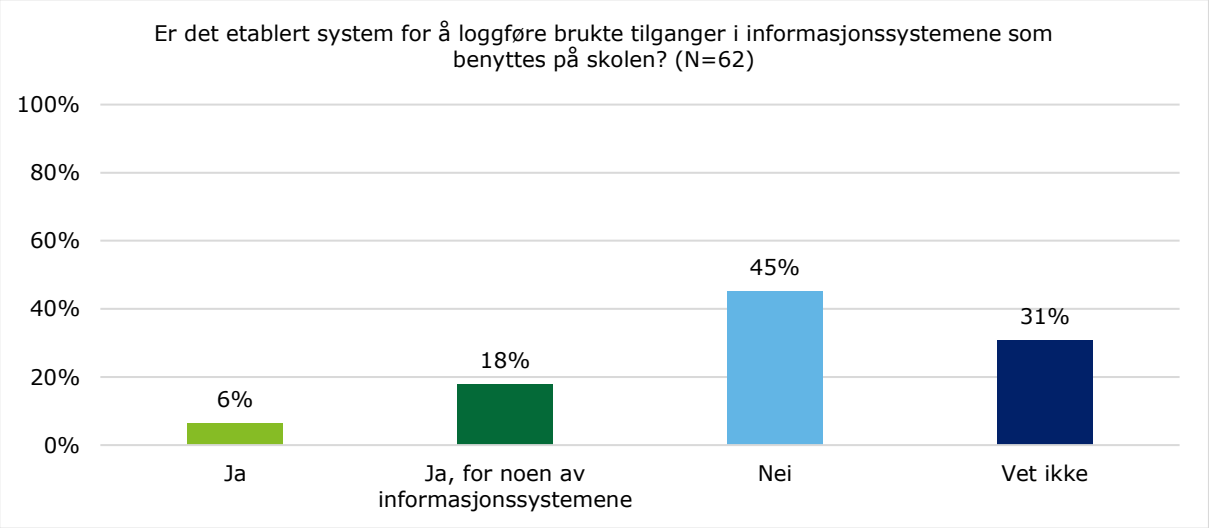
Revisjonen får opplyst at det i de fleste fagsystemene i bruk i skolesektoren, er mulig å få oversikt over hvem som har logget seg på. Slik funksjonalitet mangler etter det revisjonen får opplyst for en del mindre fagsystemer.

Revisjonen har ikke fått opplysninger om at det er etablert rutiner for å ta ut slike tilgangslogger der dette er mulig, eller at det er praksis å gjøre dette.

Revisjonen har ikke fått opplysninger om at det mulig å hente ut logger over brukte tilganger internt i fagsystemene i bruk i skolesektoren. For eksempel opplyser systemkoordinatorene at det ikke er loggføring av hvilke brukere som for eksempel har vært inne og lest i en brukermappe i Extens.[98]

I spørreundersøkelsen som ble sendt ut til alle rektorene i kommunens skoler fikk respondentene spørsmål om det er etablert system for å loggføre brukte tilganger i informasjonssystemene som benyttes på skolene:

Figur 27: System for loggføring av brukte tilganger



Som vist i figuren over svarer 45 % av rektorene som deltok i spørreundersøkelsen at det ikke er etablert et system for å loggføre brukte tilganger i informasjonssystemene ved skolene, mens 31 % svarer «vet ikke». 6 % svarer «ja» på spørsmålet, mens 18 % svarer at de har dette systemet for noen av informasjonssystemene.

På spørsmål om det er «etablert praksis å loggføre brukte tilganger i informasjonssystemene som benyttes på skolen», svarer halvparten av rektorene «nei», mens 31 % svarer «vet ikke».[99]

5.6.2 Vurdering

Det fremgår av kommunen sitt styringssystem at det er resultatenhetene som skal sørge for en dokumentert oversikt over hvem som behandler informasjon og hvor de gjør dette i skolens systemer.

Revisjonen merker seg at det for noen av de større systemene er mulig å få oversikt over hvilke brukere som logger seg på, men det fremgår ikke gjennom undersøkelsen om denne muligheten benyttes

[98] Det blir imidlertid opplyst at dersom det blir gjort endringer i innhold i Extens, kan man se hvem som har utført endringen og tidspunktet for endringen.
[99] 6 % svarer «ja» og 13 % svarer «ja, for noen av informasjonssystemene».

systematisk i skolenes informasjonssikkerhetsarbeid. Videre registrerer revisjonen at det ikke er loggføringsmuligheter over brukte tilganger i flere av de mindre systemene brukt i skolesektoren.

I spørreundersøkelsen svarer over tre av fire rektorer at det ikke er, eller at de ikke vet om det er, system for å loggføre brukte tilganger i skolens informasjonssystem.

Manglende mulighet for å loggføre brukte tilganger i de mindre systemene gjør at det ikke er mulig å avdekke eventuelle uautorisert tilganger i disse systemene. Videre mener revisjonen at manglende praksis for å hente ut tilgangslogger fra systemer der slike foreligger eller kan produseres, også reduserer sannsynligheten for at eventuelle uautoriserte påloginger i disse systemene avdekkes.

Sett i sammenheng med funnene ellers i kapittel 5, der det blant annet fremgår at over 30 % av rektorene svarer at de ikke har / ikke vet om skolen har rutiner for å hindre uautorisert tilgang til informasjonssystemene, er det revisjonens vurdering at man i skolesektoren i Bergen kommune ikke har tilstrekkelig oversikt over hvem som behandler informasjon i informasjonssystemene. Dette bryter både med generelle informasjonssikkerhetsprinsipper, og kommunens egne prosedyrer.

6. Kompetanse blant de ansatte

I dette kapittelet vil vi svare på følgende problemstilling:

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

6.1 Revisjonskriterier

Kommunen er gjennom eForvaltningsforskriften § 15 forpliktet å ha en internkontroll basert på anerkjente standarder for styringssystem for informasjonssikkerhet. Departementet har utpekt direktorat for forvaltning og IKT (Difi) som ansvarlig for å gi anbefalinger knyttet til hvilket styringssystem for informasjonssikkerhet som bør benyttes, og Difi anbefaler at offentlige virksomheter baserer seg på ISO/IEC 27001:2013. Kapittel 7.2 i standarden sier at kommunen skal:

a) fastslå hvilken kompetanse som er nødvendig for personen(e) som utfører arbeid under organisasjonens styring, og som påvirker dens informasjonssikkerhetsprestasjon;
b) sikre at disse personene har kompetanse tilegnet gjennom passende utdanning, opplæring eller erfaring;
c) der det er relevant, treffe tiltak for å erverve nødvendig kompetanse og evaluere virkningen av tiltakene som er truffet; og
d) oppbevare relevant dokumentert informasjon som bevis på kompetanse.

I merknaden til punkt 7.2, står det at «Aktuelle tiltak kan for eksempel omfatte å sørge for opplæring, veiledning eller omplassering av nåværende ansatte eller innleie av eller kontraktinngåelse med kompetente personer.»

Datatilsynet sin veileder *Internkontroll og informasjonssikkerhet*[100] omhandler blant annet oppfølging og opplæring. Her går det fram at målet med brukeropplæring er å sikre at brukerne er oppmerksomme på trusler mot personvernet og informasjonssikkerheten generelt, og at de er gitt anledning til å etterleve dette i sitt daglige arbeid. Opplæringen bør være tilpasset de ulike målgruppene sitt behov for opplæring og fordeles over tid. Brukarene bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystem for å redusere potensielle risikoer.

I tillegg til anbefalingen om opplæring av ansatte som følger av ISO-standarden, kan man utlede et krav om opplæring og kjennskap til system, rutiner og regelverk blant ansatte fra kommuneloven § 20 nr. 2 andre ledd, som sier at kommunerådet «skal sørge for at administrasjonen drives i samsvar med lover, forskrifter og overordnede instrukser, og at den er gjenstand for betryggende kontroll.» Et sentralt tiltak i ethvert internkontrollsystem vil være at det er på plass tilstrekkelig opplæring til at de ansatte er i stand til å gjennomføre sine arbeidsoppgaver i samsvar med lover, krav og forventninger.

Se vedlegg 3 for utfyllende revisjonskriterier.

6.2 Datagrunnlag

6.2.1 Opplæring av ansatte innen informasjonssikkerhet og personvern

Alle ansatte i Bergen kommune skal gjøre seg kjent med *Reglement for akseptabel bruk av IKT*, og godkjenne dette elektronisk før de får tilgang til Bergen kommunes informasjonssystemer. Revisjonen får opplyst at første gang man logger på arbeids-PC kommer *Reglement for akseptabel bruk at IKT* opp på skjermen, og man må kvittere for at man har lest og forstått dette før man kan ta i bruk maskinen. Det fremgår videre at dokumentet dukker opp på PC-skjermen ved oppstart én gang årlig, og at man må re-kvittere for å bruke maskinen videre.

[100] *Internkontroll og informasjonssikkerhet.* Datatilsynet. Publisert 23.06.2018. https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/

Ansvaret for å sørge for kompetanse innenfor informasjonssikkerhet blant ansatte er plassert hos resultatenhetslederne i kommunen gjennom *Reglement for trygg digitalisering* og *Oppdragsbeskrivelse for resultatenhetsledere.* I oppdragsbeskrivelsen fremgår det at resultatenhetslederens ansvar er å:

- sørge for at alle ansatte og andre i tjeneste for enheten kjenner kommunens reglement, instrukser og rutiner for personvern og informasjonssikkerhet
- sørge for at alle ansatte og andre i tjeneste for enheten får nødvendig og relevant opplæring for å ivareta personvern og informasjonssikkerhet

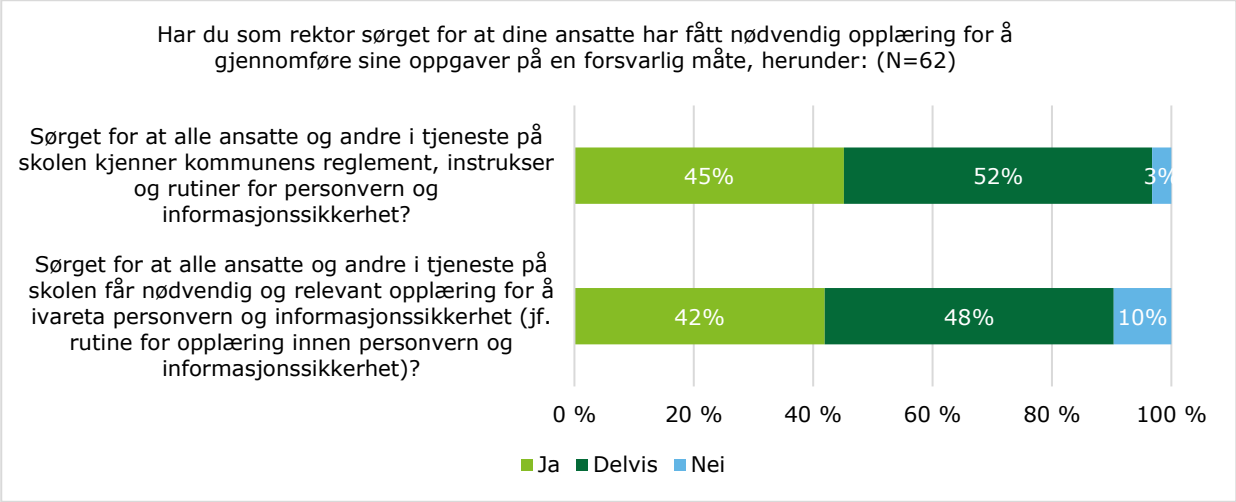
Under siste punktet vises det til *Rutine for opplæring innen personvern og informasjonssikkerhet*. Revisjonen har ikke mottatt denne rutinen, og kan heller ikke se at den foreligger på *Allmenningen*.[101]

På *Allmenningen* blir det vist til at kommunen gjennomfører nettkurs i informasjonssikkerhet der fast ansatte får e-læringskurs via e-post. Det anbefales videre at resultatenhetsledere gjennomgår e-læringskursene, oppfordrer ansatte på enheten å gjøre det samme, samt diskutere tema fra leksjonen og hvordan de er aktuelle for enheten.[102]

I spørreundersøkelsen til rektorene ble det stilt spørsmål om de har lest *Rutine for opplæring innen personvern og informasjonssikkerhet*. 42 % av rektorene svarer «nei» på dette spørsmålet mens 19 % svarer «vet ikke». 39 % av rektorene oppgir at de har lest opplæringsrutinen.

Rektorene fikk i spørreundersøkelsen videre spørsmål om de har sørget for nødvendig opplæring innen personvern og informasjonssikkerhet for sine ansatte. Svarene er gjengitt i figur 28:

Figur 28: Besørget opplæring til ansatte



Figur 28 viser at omtrent halvparten av rektorene som deltok i spørreundersøkelsen mener at de «delvis» har sørget for at de ansatte har 1) fått opplæring for å ivareta personvern og informasjonssikkerhet i henhold til opplæringsrutinen og 2) kjennskap til kommunens reglement, instrukser og rutiner for personvern og informasjonssikkerhet. 10 % av rektorene oppgir at de ikke har sørget for nødvendig og relevant opplæring for å ivareta personvern og informasjonssikkerhet.

De som svarte «delvis» eller «nei» på spørsmålene i figur 28, fikk et oppfølgingsspørsmål om hva som «kan gjøres bedre når det gjelder opplæring knyttet til informasjonssikkerhet på skolen der du er rektor». Av de 26 som svart på dette spørsmålet er det en del som etterlyser mer og bedre opplæring av rektorene, blant annet innenfor styringsdokumenter og krav til resultatenhetslederne. Noen foreslår videre at det opprettes et felles, men ikke for tidkrevende, opplæringsopplegg for de ansatte som kan brukes i alle skolene. Mange av de som svarer på oppfølgingsspørsmålet viser også til at det bør settes av mer tid til

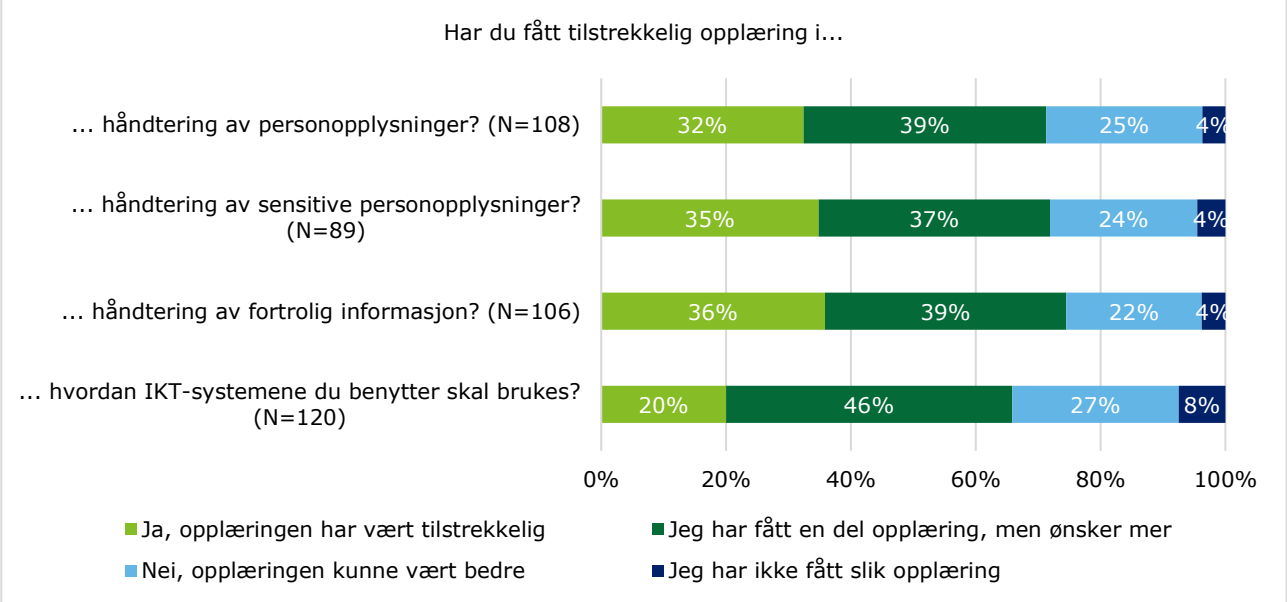
[101] Revisjonen kan ikke se at det er tilgjengeliggjort en slik rutine for opplæring under overskriften *Resultatenhetsleders ansvar – personvern og informasjonssikkerhet* og tema «opplæring av ansatte».
[102] https://allmenningen.bergen.kommune.no/ansatthjelpen/virksomhetsstyring/internkontroll/informasjonssikkerhet-og-personvern/roller-og-ansvar/resultatenhetsleders-ansvar-personvern-og-informasjonssikkerhet [sett 22.08.2019]

dette opplæringsarbeidet på skolene, og en viser konkret til at det bør gjennomføres planlagt opplæring på personalsamlinger. Et par stykker svarer at de opplever at informasjonssikkerheten har blitt bedre ved bruk av BK360.

I de åpne kommentarfeltene i spørreundersøkelsen til rektorene blir det gjentatt at det foreligger for mye og for uoversiktlig dokumentasjon og informasjon på *Allmenningen.* Videre blir det nevnt av noen at de gjennom å ha deltatt på denne spørreundersøkelsen har fått bedre oversikt over ansvarsoppgaver, rutiner og retningslinjer.

De ansatte i skolesektoren som deltok i spørreundersøkelsen fikk spørsmål om de opplever å ha fått tilstrekkelig opplæring i håndtering av ulike typer opplysninger samt bruk av IKT-systemer:[103]

Figur 29: Mottatt opplæring



Det fremgår av figur 29, at rundt én av tre svarer at de har fått tilstrekkelig opplæring knyttet til håndtering av de ulike opplysnings- og informasjonskategoriene, mens én av fem svarer at dette er tilfelle når det gjelder bruk av IKT-systemer. Resten svarer enten at de ikke har fått opplæring, at opplæringen kunne vært bedre, eller at de ønsker mer.

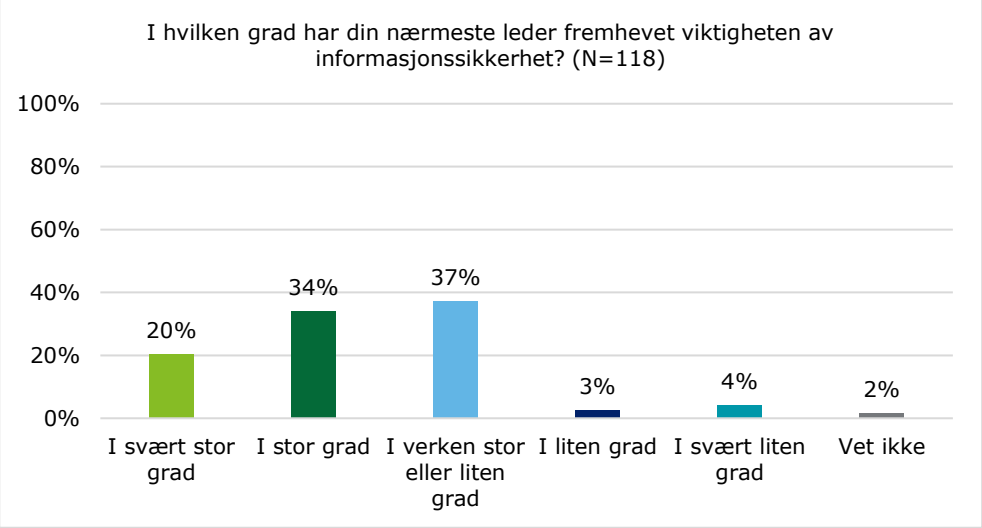
Respondentene som svarte at de ikke har fått opplæring eller ønsker mer/bedre opplæring i håndtering av informasjon og personopplysninger og/eller bruk av IKT-system, fikk et oppfølgingsspørsmål der de kunne komme med innspill til «hva kan gjøres bedre når det gjelder opplæring knyttet til informasjonssikkerhet og/eller bruk av IKT-systemer».[104] Noen svarer at det er behov for å sette av mer tid til opplæring og å få arbeide med case, prøving og feiling o.l. i forbindelse med opplæringen. Flere svarer at det er behov for hyppigere gjennomgang av tema (noen respondenter nevner at dette burde være fast tema på f.eks. områdemøter eller planleggingsdager) og hyppigere påminnelser om regler og retningslinjer. Noen etterlyser også lettere tilgjengelige retningslinjer på området og opplæring i rutiner for å melde avvik.

Videre er det en respondent som etterlyser klarere retningslinjer, like retningslinjer for samme type enheter og at ledere er oppdatert på gjeldende retningslinjer og kan drive arbeidet frem på sin enhet. En del respondenter etterlyser også mer informasjon og bedre opplæring når det gjelder BK360.

[103] Det er bare respondentene som tidligere i spørreundersøkelsen har oppgitt at de behandler personopplysninger i arbeidshverdagen som får spørsmål om opplæringen knyttet til håndteringen av denne typen informasjon. Tilsvarende for spørsmål om sensitive personopplysninger og fortrolig informasjon.
[104] N=28 (tre av kommentarene var blanke eller «vet ikke»/ «ingen spesiell mening» og ble dermed fjernet fra utvalget)

Respondentene fikk videre spørsmål om i hvilken grad nærmeste leder har fremhevet viktigheten av informasjonssikkerhet. Svarene fremgår i figur 30:

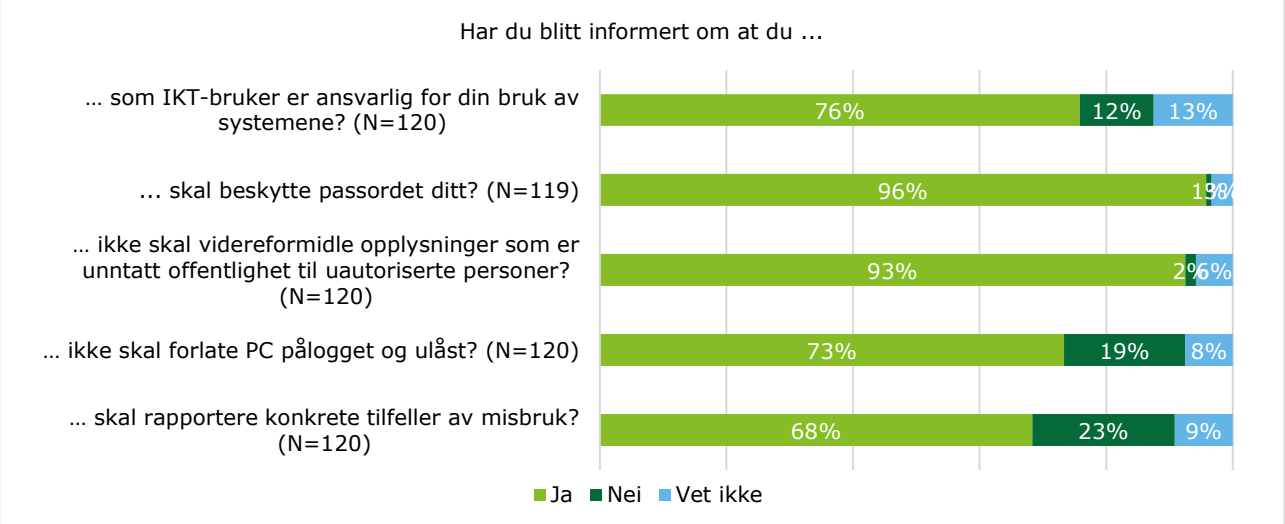
Figur 30: Viktigheten av informasjonssikkerhet



Som fremstilt i figuren over, svarer de fleste at nærmeste leder enten i «svært stor grad» eller «i stor grad» har fremhevet viktigheten av informasjonssikkerhet; til sammen 7 % oppgir at dette «i liten grad» eller «i svært liten grad» har blitt fremhevet av nærmeste leder.

Videre fikk respondentene i spørreundersøkelsen spørsmål om hvilken informasjon de eventuelt har mottatt når det gjelder informasjonssikkerhetspraksis. Svarene fremgår i figur 31 under:

Figur 31: Informasjon om informasjonssikkerhetspraksis



Som gjengitt i figuren over svarer majoriteten av respondentene «ja» på samtlige delspørsmål. 23 % av respondentene svarer at de ikke har blitt informert om at de skal rapportere konkrete tilfeller av misbruk, mens 9 % svarer «vet ikke» på samme spørsmål. 27 % av respondentene svarer at de ikke har blitt informert eller ikke vet om de har blitt informert om at de ikke skal forlate PC pålogget og ulåst. 25 % svarer at de ikke har blitt informert eller ikke vet om de har blitt informert om at de som IKT-bruker er ansvarlig for sin bruk av systemene. Videre er det 4 % som oppgir at de ikke har eller ikke vet om de har blitt informert om at de skal beskytte passordet sitt. Omtrent 8 % svarer at de ikke har/ikke vet om de har fått informasjon om å ikke videreformidle opplysninger som er unntatt offentligheten til uautoriserte personer.

6.2.2 Kompetanse hos de ansatte

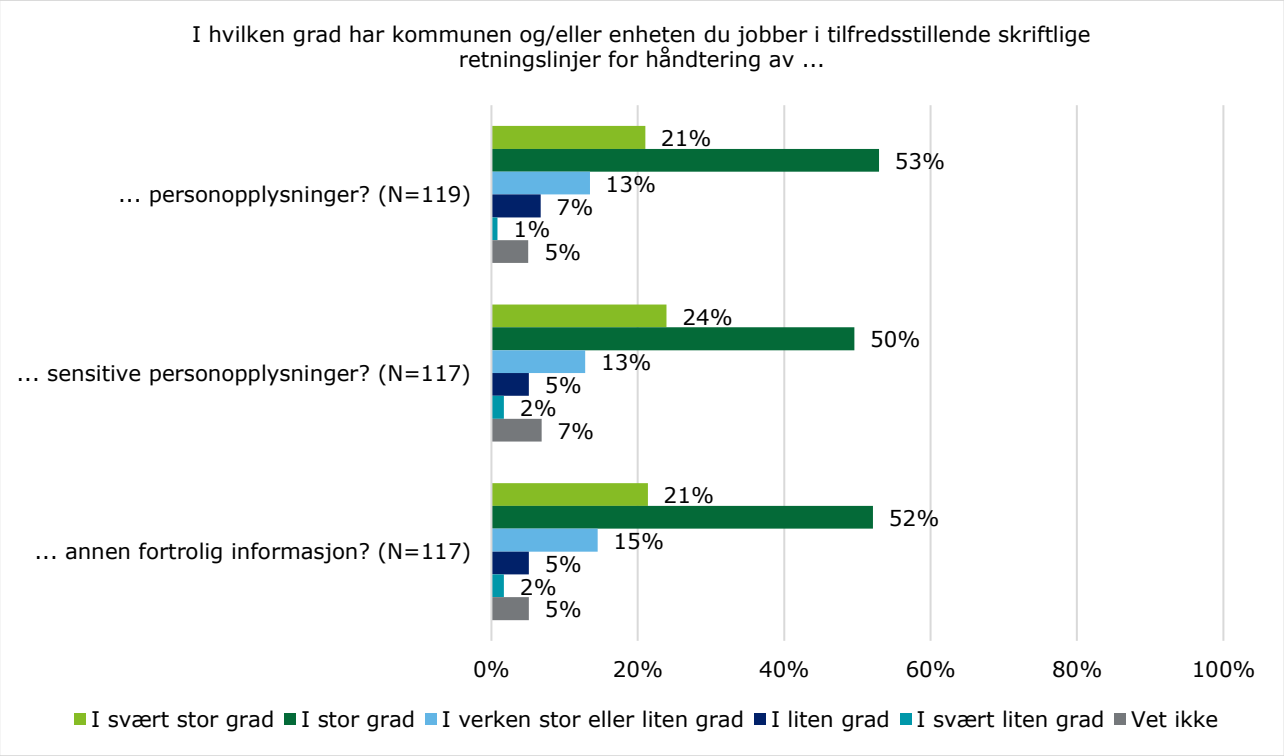
Kjennskap til rutiner og retningslinjer

I spørreundersøkelsen som ble sendt ut til et utvalg ansatte i Bergen kommune svarer nesten 90 % av respondentene fra skolesektoren at de «behandler personopplysninger, sensitive personopplysninger og/eller kommer i kontakt med annen fortrolig informasjon i sitt arbeid».[105]

Deltakerne fikk videre spørsmål om de vet hvor man finner «rutiner og retningslinjer for håndtering av personopplysninger, sensitive personopplysninger og/eller annen fortrolig informasjon»; her svarer 40 % av respondentene «nei».[106] Rektorene som deltok i spørreundersøkelse fikk tilsvarende spørsmål; 8 % av rektorene svarer «nei» på dette spørsmålet mens 92 % svarer «ja». [107]

Deltakerne i spørreundersøkelsen fikk også spørsmål om i hvilken grad kommunen og/eller enheten de jobber i har tilfredsstillende retningslinjer for håndtering av personopplysninger, sensitive person-opplysninger og annen fortrolig informasjon. Fordelingen av svarene er fremstilt i figuren under:

Figur 32: Tilfredsstillende retningslinjer for håndtering av konfidensiell informasjon



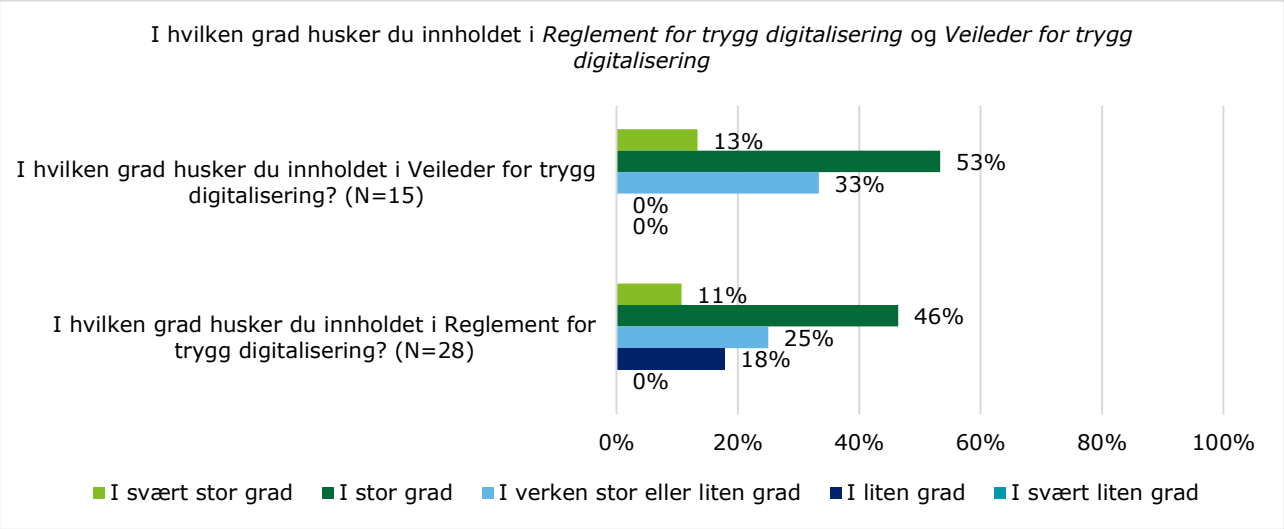
Figur 32 viser at nesten tre fjerdedeler[108] av respondentene svarer at kommunen og/eller enheten «i stor grad» eller «i svært stor grad» har tilfredsstillende skriftlige rutiner for å håndtere personopplysninger, sensitive personopplysninger og annen fortrolig informasjon. 5 % av respondentene oppgir at det «i liten grad» er skriftlige retningslinjer for håndtering av sensitive personopplysninger og annen fortrolig informasjon, mens 7 % oppgir at dette «i liten grad» er tilfelle for personopplysninger.

Respondentene fikk videre spørsmål om de har lest *Reglement for trygg digitalisering*[109] og *Veileder for trygg digitalisering.*[110] Halvparten av respondentene svarer at de ikke har lest reglementet og litt over halvparten oppgir at de ikke har lest veilederen. Rundt 30 % av respondentene svarer «vet ikke» på begge spørsmålene.

[105] N=120.
[106] N=118.
[107] N=62.
[108] 73 % -74 %.
[109] N=120
[110] N=119

De respondentene som oppgir at de har lest *Reglement for trygg digitalisering* og *Veileder for trygg digitalisering* fikk spørsmål om i hvilken grad de husker innholdet i disse dokumentet. Som fremstilt i figur 33 under svarer 18 % at de «i liten grad» husker innholdet i *Reglement for trygg digitalisering*, mens 25 % oppgir at de «i verken stor eller liten grad» kan huske innholdet i dette dokumentet.

Figur 33: Husker regler og veiledning

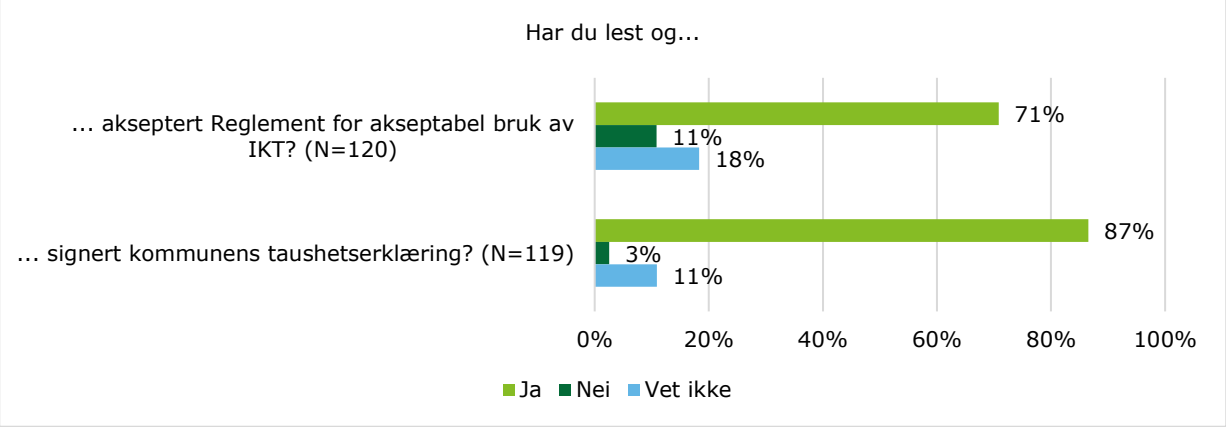


33 % av de som oppgir at de har lest *Veileder for trygg digitalisering* svarer at de «i verken stor eller liten grad» husker innholdet i dette dokumentet, mens de resterende 66 % svarer at de «i svært stor grad» eller «i stor grad» husker innholdet.

De respondentene som svarer at de enten «i svært stor grad», «i stor grad» eller «i verken stor eller liten grad» husker innholdet i *Reglement for trygg digitalisering*[111] og *Veileder for trygg digitalisering*[112], fikk et oppfølgingsspørsmål på i hvilken grad innholdet i dokumentet var forståelig for dem. Om lag tre av fire respondenter svarer at innholdet «i svært stor grad» eller «i stor grad» var forståelig for dem[113]

Respondentene fikk videre spørsmål om de har lest og akseptert *Reglement for akseptabel bruk av IKT* og om de har lest og signert kommunens taushetserklæring. Svarene er fremstilt i figur 34:

Figur 34: Lest og akseptert/signert sentrale dokumenter



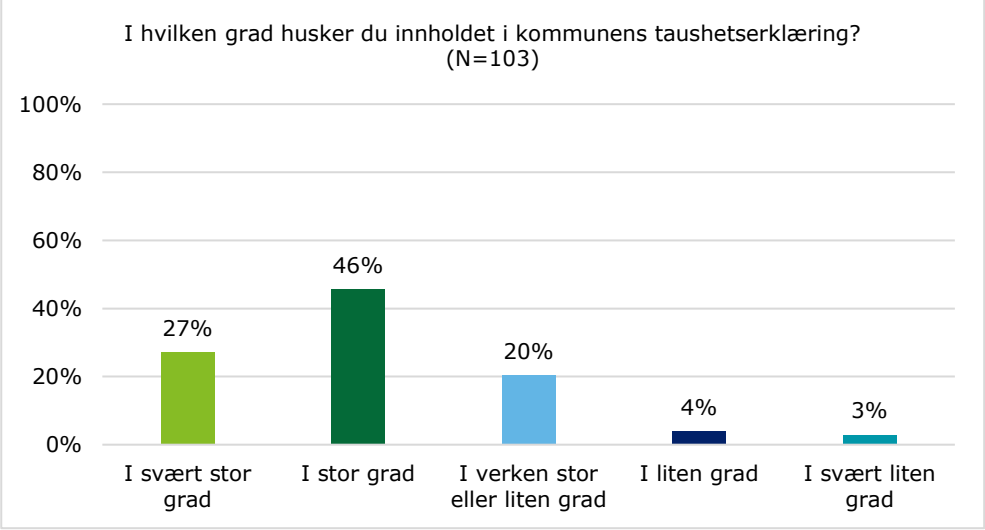
[111] N=22
[112] N=14
[113] 23 % svarer at innholdet i Reglement for trygg digitalisering «i verken stor eller liten grad» var forståelig for dem mens de resterende 77 % oppgir at innholdet «i svært stor grad» eller «i stor grad» var forståelig. Nesten 80 % svarer at innholdet i Veileder for trygg digitalisering «i svært stor grad» eller «i stor grad» var forståelig, mens rundt 20 % svarer at innholdet «i verken stor eller liten grad» var forståelig for dem.

Som vist i figuren over svarer nesten 30 % av respondentene at de ikke har eller ikke vet om de har lest og akseptert *Reglement for akseptabel bruk av IKT*, mens 14 % oppgir at de ikke har eller ikke vet om de har lest og signert kommunens taushetserklæring.

Respondentene som svarer «ja» på spørsmålet om de har lest og akseptert *Reglement for akseptabel bruk av IKT* fikk oppfølgingsspørsmål om i hvilken grad de husket innholdet i dokumentet, og i så tilfelle om innholdet i dokumentet var forståelig for dem. Omtrent to av fem respondentene svarer at de i stor eller svært stor grad husker innholdet.[114] Størstedelen av respondentene som oppgir at de husker innholdet i reglementet[115] svarer videre at innholdet i reglementet er forståelig for dem.[116]

Respondentene som oppgir at de har lest og signert kommunens taushetserklæring fikk et oppfølgingsspørsmål om i hvilken grad de husker innholdet i denne:

Figur 35: Kjennskap til kommunens taushetserklæring



Som fremstilt i Figur 35 oppgir de fleste av respondentene at de husker innholdet i taushetserklæringen, mens 7 % «i liten grad» eller «i svært liten grad» husker innholdet i denne. 20 % svarer at de «i verken stor eller liten grad» husker innholdet i taushetserklæringen.

Melding av avvik knyttet til informasjonssikkerhet

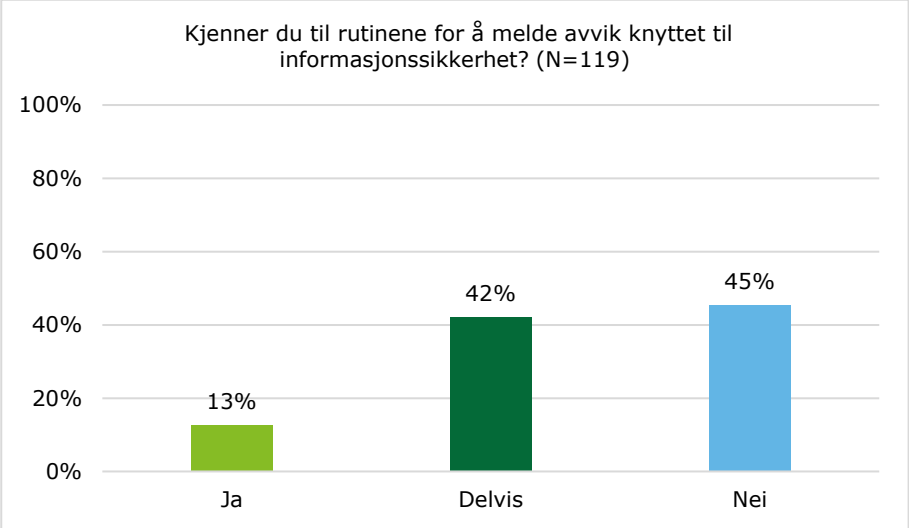
De ansatte i skolesektoren som deltok i spørreundersøkelsen fikk spørsmål om de kjenner til rutinene for å melde avvik knyttet til informasjonssikkerhet:

[114] N=84. 13 % oppgir at de i liten eller svært liten grad husker innholdet. 44 % svarer at de «i verken stor eller liten grad» husker innholdet

[115] Respondentene som svarte «i svært stor grad», «i stor grad» og «i verken stor eller liten grad».

[116] N=68. «I hvilken grad er innholdet i *Reglement for akseptabel bruk av IKT* forståelig for deg?» 10 % svarer «i svært stor grad», 59 % svarer «i stor grad» og 31 % svarer «i verken stor eller liten grad». Ingen av respondentene svarer «i liten grad» eller «i svært liten grad».

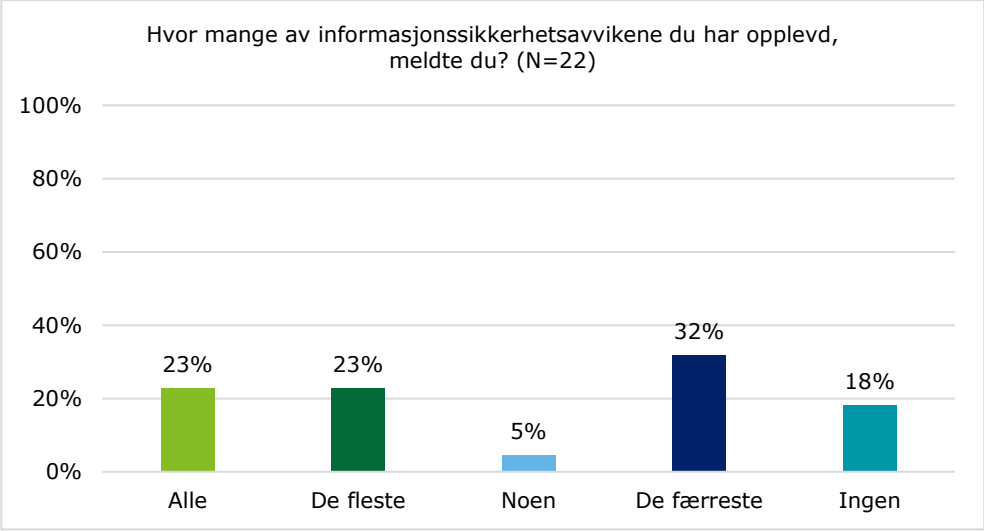
Figur 36: Kjennskap til avviksrutiner knyttet til informasjonssikkerhet



Som fremstilt i figur 36 svarer 45 % av respondentene at de *ikke* kjenner rutinene for å melde avvik knyttet til informasjonssikkerhet. 42 % av respondentene fra skolesektoren svarer at de «delvis» kjenner disse avviksrutinene.

Respondentene fikk videre spørsmål om de har «opplevd ett eller flere informasjonssikkerhetsavvik». Rundt 19 % svarte «ja», 60% «nei» og 22 % «vet ikke».[117] De 22 som svarte «ja» på dette spørsmålet fikk et oppfølgingsspørsmål på hvor mange av de opplevde informasjonssikkerhetsavvikene de meldte:

Figur 37: Meldte avvik

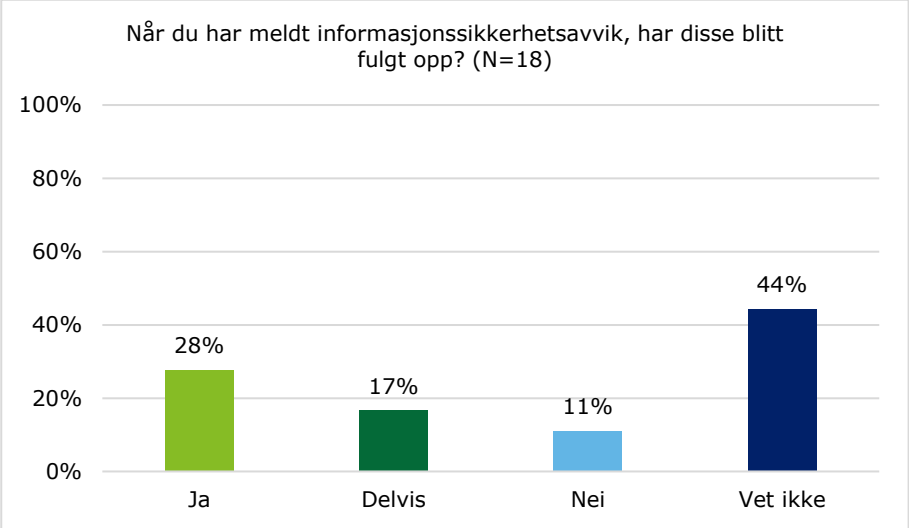


Figur 37 viser at 32 % av de som oppgir at de har opplevd informasjonssikkerhetsavvik har meldt fra om «de færreste» av disse, mens 18 % svarer at de meldte «ingen» av de opplevde avvikene. 5 % av respondentene svarer at de har meldt «noen» av informasjonssikkerhetsavvikene de har opplevd.

Respondentene 18 som ikke svarte «ingen» på spørsmålet, fikk et oppfølgingsspørsmål knyttet til oppfølging av avvikene (se figur 37):

[117] N=119

Figur 38: Oppfølging av meldte informasjonssikkerhetsavvik

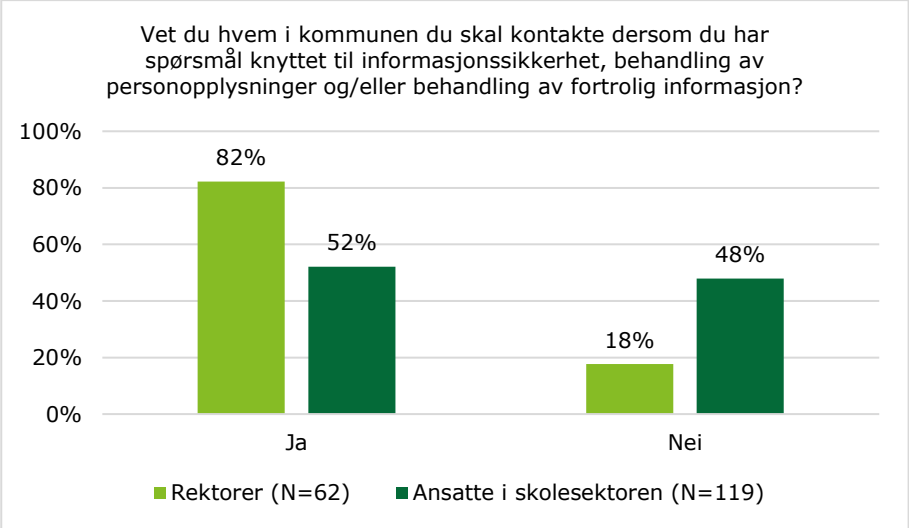


Som vist i figuren svarer 44 % av respondentene at de ikke vet om informasjonssikkerhetsavvikene de har meldt har blitt fulgt opp. 11 % svarer at de meldte avvikene ikke har blitt fulgt, mens 17 % svarer at avvikene «delvis» har blitt fulgt opp.

Kjennskap til kontaktpersoner i kommunen

Respondentene i begge spørreundersøkelsen fikk spørsmål om de vet hvem i kommunen de skal kontakte dersom de har «spørsmål knyttet til informasjonssikkerhet, behandling av personopplysninger og/eller behandling av fortrolig informasjon»:

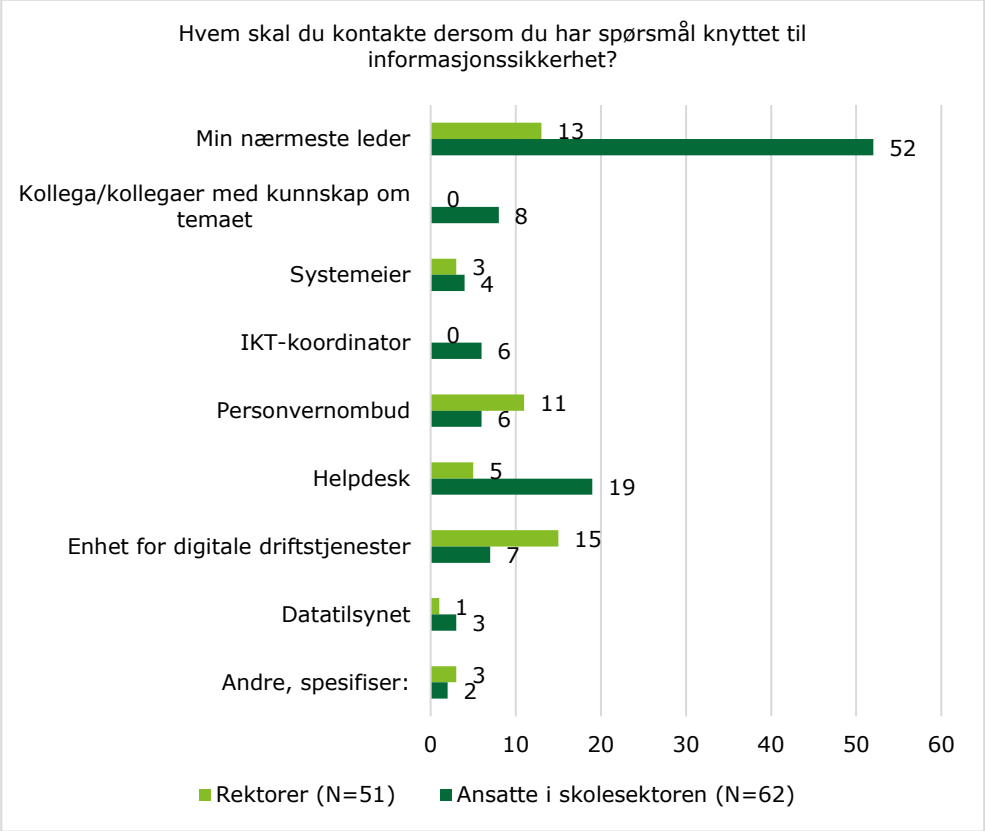
Figur 39: Kjennskap til hvem som kontaktes ved spørsmål om informasjonssikkerhet og personvern



Figur 39 viser at 48 % av de ansatte i skolesektoren svarer at de *ikke* vet hvem de skal kontakte med spørsmål som dreier seg om informasjonssikkerhet og behandling av personopplysninger og/eller fortrolig informasjon, mens 18 % av rektorene svarer «nei» på samme spørsmål.

De respondentene som svart «ja» på spørsmålet som er gjengitt i figur 39 fikk et oppfølgingsspørsmål der de kunne svare på hvem de vil kontakte med disse spørsmålene:

Figur 40: Hvem kontaktes ved spørsmål om informasjonssikkerhet og personvern[118]



Som vist i figur 40 svarer 52 av de 62 respondentene som er ansatte i skolesektoren at de vil kontakte nærmeste leder med spørsmål om informasjonssikkerhet. 19 av de ansatte og 5 av rektorene ville videre ha kontaktet Helpdesk med slike spørsmål, mens 11 av rektorene og 6 av de ansatte ville kontaktet personvernombud. Seks av de ansatte svarer at de ville ha kontaktet IKT-koordinator, mens ingen av rektorene oppgir dette som mulig alternativ.

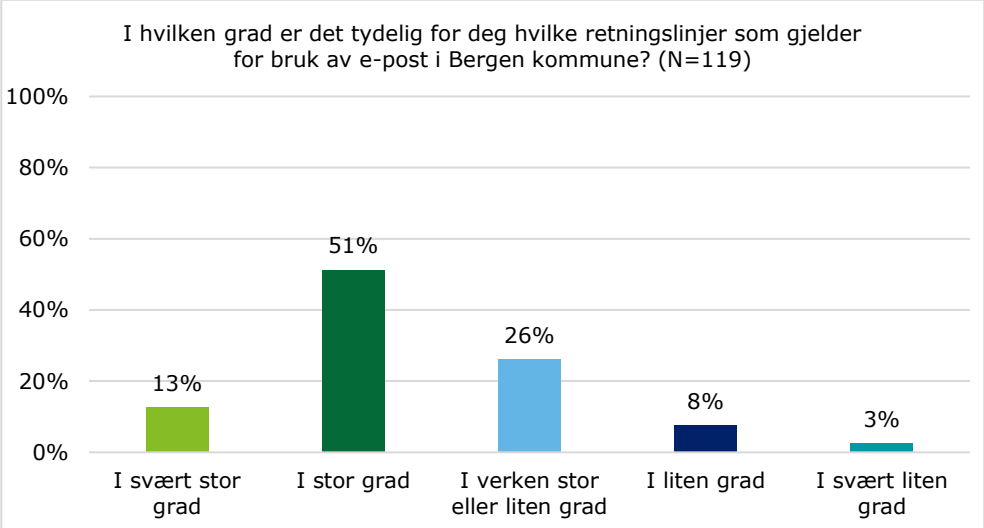
De to ansatte i skolesektoren som har svart «andre, spesifiser» utdyper at de vil kontakte henholdsvis media og seksjon for internkontroll dersom de har spørsmål knyttet til informasjonssikkerhet, mens de tre rektorene som oppgir «andre» utdyper at de enten ville ha kontaktet avdeling for personvern og informasjonssikkerhet, digitalisering og innovasjon, brukt *Allmenningen* eller spurt en kollega eller nærmeste leder.

6.2.3 Trygg e-postbruk – kompetanse og etterlevelse

I spørreundersøkelsen fikk respondentene spørsmål om de opplever at det er tydelig hvilke retningslinjer som gjelder for bruk av e-post i Bergen kommune. Svarene er presentert i figur 41:

[118] Respondentene kunne krysse av for flere alternativ på dette spørsmålet, og svarene er derfor ikke prosentuert.

Figur 41: Tydelige retningslinjer for bruk av e-post



Som fremstilt i figur 41 svarer 11 % av respondentene at det «i liten grad» eller «i svært liten grad» er tydelig hva som er gjeldende retningslinjer for bruk av e-post. 26 % av respondentene oppgir at de opplever at retningslinjene for e-postbruk «i verken stor eller liten grad» er tydelige.

For å teste om og i hvilken grad ansatte i skolen i Bergen kommune praktiserer trygg e-postbruk, gjennomførte revisjonen et nettfiskeforsøk (phising). Totalt fikk 13 365 ansatte i Bergen kommune tilsendt en falsk e-post, hvorav 3 351 var ansatt i skolesektoren. Testen var utformet for å måle i hvor stor utstrekning mottagerne trykker på en lenke i en e-post fra en ukjent og mistenkelig avsender, og hvorvidt de oppgir sensitive opplysninger som brukernavn og passord. I tillegg bidrar nettfiskeforsøket til praktisk læring og bevisstgjøring blant de ansatte om egen e-postbruk, noe som er årsaken til at målgruppen til forsøket har vært alle fast ansatte i kommunens skoler.[119]

Det er viktig å understreke at formålet med testen var å undersøke om *ansatte i skolen* i Bergen kommune praktiserer trygg e-postbruk, og ikke å teste hvordan Bergen kommune som *organisasjon* responderer i situasjoner der ansatte utsettes for nettfiskeangrep eller lignende, eller hvorvidt kommunens *tekniske* sikkerhetsmekanismer fungerer etter hensikten.

Bergen kommune sine tekniske sikkerhetsmekanismer måtte slås av for at nettfiskeforsøket skulle kunne gjennomføres. Blant annet måtte avsenderadressen registrere i kommunen sine spam-filter for at e-posten skulle nå frem til de ansatte. I tillegg avstod Helpdesk fra å sperre lenken i e-posten, noe de rutinemessig ville gjort under et autentisk angrep som avdekkes.

Bergen kommune har også rutiner for å varsle sine ansatte om pågående angrep når slike blir avdekket. Blant annet har kommunen som rutine å varsle IKT-kontakter per SMS om slike hendelser, og det skal alltid legges ut informasjon på *Allmenningen* om pågående hendelser av denne typen. Gitt formålet med testen, ble kommunen bedt om å ikke iverksette slike organisatoriske tiltak.[120] Hadde kommunen rutinemessig respondert og informert alle ansatte om at de ikke skulle trykke på lenken i e-posten, ville det kunne redusert antallet ansatte som trykket på lenken og oppga sitt brukernavn og passord, noe som dermed ikke ville gitt et riktig bilde på hvorvidt den enkelte *ansatte* praktiserer trygg e-postbruk.[121] Det er

[119] Ansatte som jobber i kommunalt AS, er politikere, har en stillingsprosent under 40 %, er ekstrahjelper, vikarer, o.l., eller har en av stillingstypene assistenter, renholdere, studenter og pensjonister, er utelukket fra forsøket.
[120] Ved feiltakelse ble det gitt ulike beskjeder da nettfiskeforsøket hadde kommet i gang, noe som medførte at det i en kortere periode ble opplyst på intranettet til Bergen kommune at det var pågående et nettfiskeforsøk, og at ansatte ikke skulle trykke på lenken. Dette kan i noen grad ha påvirket de ansatte som leste beskjeden på intranettet til ikke å trykke på lenken i e-posten, og det kan derfor være at antallet som trykket på lenket og oppga passord og brukernavn ville vært høyere dersom denne beskjeden ikke ble lagt ut.
[121] Kommunen opplyser at flere ansatte i etterkant av forsøket har fortalt at de tok sjansen på å åpne e-posten, nettopp fordi det ikke var varslet i kommunens interne kanaler om at det var pågående et angrep.

avgjørende at den enkelte ansatte praktiserer trygg e-postbruk, uavhengig av hvilke responsrutiner og -praksis organisasjonen har på systemnivå, og hvilke tekniske sikkerhetsmekanismer som er på plass. Et reelt nettfiskeangrep går ikke nødvendigvis bredt ut i en organisasjon, men sendes gjerne til enkeltpersoner eller mindre utvalg av ansatte. Dette kan både være for å tilpasse angrepet ytterligere og slik øke sannsynligheten for suksess, men også for å redusere risikoen for at forsøket avsløres og organisasjonen responderer slik Bergen kommune har som rutine.[122]

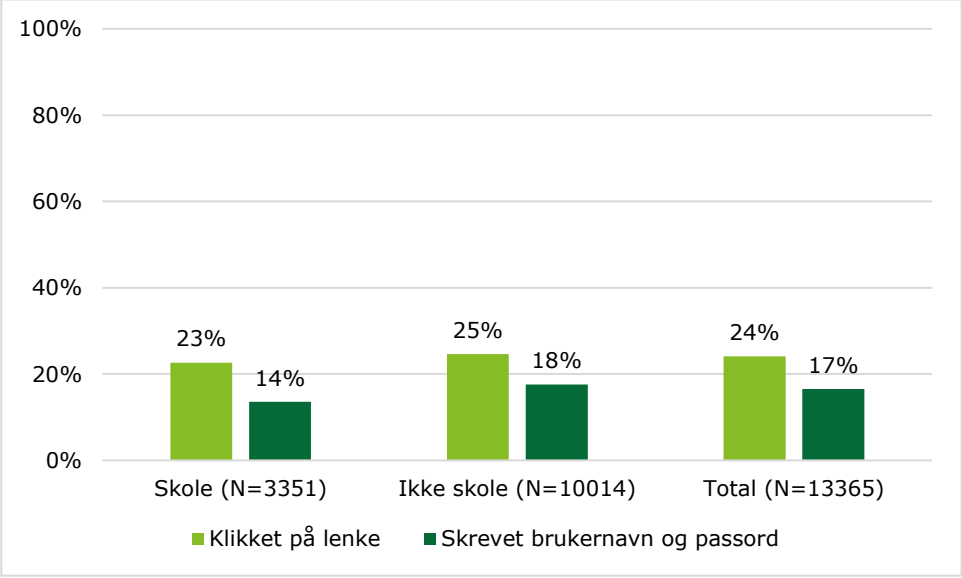
Målgruppen i nettfiskeforsøket mottok 15. mai en e-post fra avsenderen «Dcure Global» med invitasjon til en etikkundersøkelse for Bergen kommune. For å besvare undersøkelsen ble mottakerne bedt om å trykke på en lenke i e-posten.

Nettfiskeforsøket var utformet slik at det skulle fremstå som troverdig, blant annet ved å inneholde kommunens logo og omhandle et tema som angår de fleste ansatte i kommunen. E-posten inneholdt imidlertid også elementer som gjorde det mulig for mottagerne å avsløre testen; dette gjaldt eksempelvis den ukjente avsenderen og avsenderadressen, samt adressen til selve nettsiden. I tillegg var ordlyden i invitasjonen, samt selve designet på nettsiden, utformet for å kunne vekke en viss mistanke om at e-posten kunne være falsk.

Ansatte som klikket på lenken i e-posten, ble videresendt til en nettside der de ble bedt om å taste inn sitt brukernavn og passord for å svare på selve etikkundersøkelsen. Ansatte som gjorde dette, kom videre til en nettside der de ble informert om at de hadde blitt utsatt for et nettfiskeforsøk, og som lenket til rutiner og retningslinjer for informasjonssikkerhet i Bergen kommune.

Av de 13 365 ansatte som fikk nettfiskeforsøkseposten, trykket 3 226 på lenken. Av disse skrev 2 213 inn sitt brukernavn og passord. Med andre ord valgte nesten én av fire (litt over 24 %) å trykke på lenken i e-posten, mens 16,5 % oppgav sitt brukernavn og passord. Av de 3 351 ansatte i skolesektoren som ble tilsendt e-posten, trykket 759 på lenken, og 455 av disse oppgav sitt brukernavn og passord. Dette betyr at om lag 23 % trykket på lenken, og 14 % oppgav brukernavn og passord. Figur 42 viser resultatene av nettfiskeforsøket fordelt mellom skolesektoren, resten av kommunen, og totalt:

Figur 42: Resultater nettfiskeforsøk



[122] Kommunen publiserte en nyhetssak om nettfiskeforsøket på *Allmenningen* etter at forsøket var avsluttet.

6.3 Vurdering

Opplæring

Undersøkelsen viser at ansvaret for opplæring av ansatte innenfor informasjonssikkerhet er plassert hos rektor som resultatenhetsleder og videre at kommunen stiller som vilkår for bruk av IKT-systemene at ansatte har lest og akseptert *Reglement for akseptabel bruk av IKT*. I tillegg er det, som det gjennomgående vises til i rapporten, tilgjengeliggjort informasjon og veiledningsmateriell innenfor ulike informasjonssikkerhetstema for de ansatte. Revisjonen mener på denne bakgrunn at kommunen har lagt til rette for at ansatte kan tilegne seg kunnskap og kompetanse knyttet til informasjonssikkerhet og personvern.

I spørreundersøkelsen kommer det imidlertid frem at en relativt stor del av rektorene ikke kjenner til sentrale opplæringsrutiner; 42 % av rektorene oppgir å ikke ha lest *Rutine for opplæring innen personvern og informasjonssikkerhet,* mens 19 % ikke vet om de har lest denne. Videre fremgår det at omtrent halvparten av rektorene oppgir å bare delvis ha besørget nødvendig opplæring for sine ansatte knyttet til informasjonssikkerhet slik de er forpliktet til. Dette reflekteres i svar på spørsmål om mottatt opplæring, der over 60 % av respondentene oppgir å ikke ha fått tilstrekkelig opplæring knyttet til personvern og informasjonssikkerhet, og 80 % ønsker mer opplæring knyttet til bruk av IKT-systemer.

Revisjonen merker seg også at informasjon om god informasjonssikkerhetspraksis ikke har nådd ut til alle ansatte i skolesektoren; totalt 25 % oppgir at de ikke vet om de har blitt eller at de ikke har blitt informert om ansvaret de har for bruk av IKT-systemene, 27 % oppgir at de ikke vet om de har blitt eller at de ikke har blitt informert om at de ikke skal forlate PC pålogget og ulåst, og 32 % oppgir at de ikke vet om de har blitt eller at de ikke har blitt informert om at de skal rapportere konkrete tilfeller av misbruk.

Basert på funnene i undersøkelsen, er det revisjonen sin vurdering at Bergen kommune ikke fullt ut er i samsvar med krav og anbefalinger om kommunen sitt ansvar for å sikre tilstrekkelig informasjons-sikkerhetskompetanse blant de ansatte gjennom opplæringstiltak (f.eks. ISO27001:2013 punkt 7.2).

Dette medfører økt sannsynlighet for at de ansatte ikke har tilstrekkelig kompetanse innen informasjons-sikkerhet, noe som øker risikoen for brudd på regelverket som gjelder for behandling av personopplysninger og for informasjonssikkerhet generelt. Funnene knyttet til informasjonssikkerhetskompetanse og –praksis (se avsnitt under og kapittel 4) tyder videre på at denne risikoen har gjort seg gjeldende.

Kompetanse

Undersøkelsen viser at majoriteten av respondentene behandler personopplysninger, sensitive person-opplysninger eller annen fortrolig informasjon i sitt arbeid. Likevel svarer 40 % av respondentene at de ikke vet hvor de finner kommunen sine retningslinjer for hvordan slike opplysninger skal håndteres. 8 % av rektorene svarer «nei» på samme spørsmålet.

Revisjonen merker seg videre at om lag 30 % av respondentene ikke vet om de har lest *Reglement for akseptabel bruk av IKT*. Dette til tross for at ansatte må kvittere for at de har lest dette for å få tilgang til egen datamaskin for første gang, samt én gang per år for å beholde tilgang til kommunens informasjonssystemer. I tillegg svarer bare rundt en av fem respondenter at de har lest Reglement for trygg digitalisering, kommunens overordnete reglement for informasjonssikkerhet, mens litt over halvparten svarer at de ikke har lest Veileder for trygg digitalisering. Kun 13 % svarer «ja» på spørsmålet om de kjenner rutinene for å melde avvik knyttet til informasjonssikkerhet.

Det fremgår videre i spørreundersøkelsen at av respondentene som har opplevd informasjonssikkerhets-avvik, meldte halvparten «ingen» eller «de færreste» av disse, og videre at av respondentene som har meldt avvik, svarer 11 % at de meldte avvikene ikke ble fulgt opp, og 44 % at de ikke vet om avvikene ble fulgt opp. Revisjonen vil i den forbindelse peke på at manglende avviksmeldinger øker risikoen for at svakheter i system og organisasjon ikke blir avdekket og derfor heller ikke rettet, og videre at manglende eller opplevd manglende oppfølging av innmeldte avvik kan dempe motivasjonen for å melde avvik, og slik øke risikoen for at nye avvik ikke blir meldt.

Revisjonen merker seg videre at nesten halvparten av respondentene svarer at de *ikke* vet hvem de skal kontakte med spørsmål som dreier seg om informasjonssikkerhet og behandling av personopplysninger og/eller fortrolig informasjon, mens 18 % av rektorene svarer «nei» på samme spørsmål.

Resultatene fra nettfiskeforsøket viser videre at ansatte i skolesektoren i Bergen kommune har en svak informasjonssikkerhetspraksis; nesten én av fire (23 %) valgte å trykke på lenken i e-posten, og 14 % oppgav sitt brukernavn og passord. Bergen kommune har tekniske sikkerhetsmekanismer som skal redusere risikoene knyttet til nettfiske (disse måtte slås av for at nettfiskeforsøket skulle kunne gjennomføres). Kommunen har også rutiner knyttet til hendelseshåndtering, som også ble stanset for å tillate gjennomføringen av forsøket. Revisjonen mener likevel at kommunen må sikre at ansatte har tilstrekkelig kompetanse for å håndtere denne typen sikkerhetsrisikoer.

Basert på funnene i undersøkelsen, er det revisjonen sin vurdering at ikke alle ansatte i skolesektoren i Bergen kommune har tilstrekkelig kjennskap til retningslinjer og rutiner for informasjonssikkerhet. Revisjonen er oppmerksom på at gjeldende styringssystem for informasjonssikkerhet relativt nylig ble utarbeidet og implementert, og videre at det er planer om å tilby de ansatte ytterligere opplæring. Likevel mener revisjonen at det på revisjonstidspunktet er risiko for at kommunen ikke er i samsvar med regelverk og anbefalinger på området på grunn av manglende kompetanse blant de ansatte i skolesektoren.

Sett i sammenheng med funnene for eksempel i kapittel 4 er det videre revisjonen sin vurdering at de ansatte i skolesektoren i Bergen kommune ikke i tilstrekkelig grad etterlever retningslinjer og rutiner for informasjonssikkerhet, og videre at informasjonssikkerhetspraksisen blant de ansatte bryter med flere grunnleggende informasjonssikkerhetsprinsipp.

7. Konklusjon og anbefalinger

I denne forvaltningsrevisjonen har Deloitte undersøkt hvordan informasjonssikkerheten er ivaretatt i skolesektoren i Bergen kommune. Fokuset i forvaltningsrevisjonen har vært på etterlevelse av kommunens styringssystem for informasjonssikkerhet.

Rutiner og ansvar for informasjonssikkerhet

Gjennom styringssystemet for personvern og informasjonssikkerhet og tilhørende oppdragsbeskrivelser, mandater og veiledere, har Bergen kommune skriftliggjort ansvar og oppgaver knyttet til informasjonssikkerhet.

Undersøkelsen viser imidlertid at rolle- og ansvarsfordelingen knyttet til informasjonssikkerhet i skolesektoren verken oppleves som tydelig eller som hensiktsmessig organisert. Informasjonssikkerhetsarbeidet sentralt i skolesektoren i Bergen kommune preges av en uformell rolle- og ansvarsdeling, noe som gir økt risiko for uklarheter og manglende oppfølging av informasjonssikkerhetsarbeide, med tilhørende risiko for brudd på informasjonssikkerheten. Revisjonen mener at informasjonssikkerhetsbruddet høsten 2019 viser at slik risiko har gjort seg gjeldende i kommunen.

Videre viser undersøkelsen at det ute i skolene ikke er etablert klare rutiner og ansvarsforhold med hensyn til informasjonssikkerhet. I tillegg kommer det frem at det som er etablert av rutiner og ansvarsforhold er delvis avvikende fra kommunens styringssystem for informasjonssikkerhet. Funn i undersøkelsen viser også at roller og ansvar knyttet til informasjonssikkerhet blir oppfatte som uklart for en relativt stor andel av rektorene ved skolene, samt at informasjonssikkerhetsoppgaver som påhviler rektorene bare delvis blir gjennomført.

Revisjonen er oppmerksom på at det er relativt kort tid siden gjeldende styringssystem for personvern og informasjonssikkerhet ble utarbeidet og implementert i kommunen, og videre at byrådsavdelingen nylig er omorganisert. Dette er begge momenter som kan være med å forklare at rutiner og ansvarsforhold i skolesektoren når det gjelder informasjonssikkerhet ikke fremstår som entydige eller klare. Revisjonen ser det i den sammenheng som positivt at det er opprettet en stilling som informasjonssikkerhetsrådgiver i skolesektoren,[123] at det er etablert en seksjon for HR, digitalisering og virksomhetsstyring som blant annet skal arbeide med å ivareta IKT-sikkerheten i byrådsavdelingen og skolesektoren, og at områdelederne i ny organisering er tiltenkt en rolle for å legge til rette for at skolene etterlever styringssystemet for informasjonssikkerhet og personvern.

Konfidensialitet

Bergen kommune har formalisert ansvar og oppgaver knyttet til å **hindre uautorisert innsyn i konfidensielle opplysninger** gjennom styringssystemet for personvern og informasjonssikkerhet med tilhørende dokumenter.

Informasjonssikkerhetsbruddet knyttet til innsyn i konfidensielle opplysninger i forbindelse med implementeringen av Vigilo, tyder på at verken system, rutiner eller ansvars- og oppgavefordeling for å hindre uautorisert innsyn i konfidensielle opplysninger er tilstrekkelig ivaretatt i skolesektoren i Bergen kommune.

Det er nylig implementert tekniske tiltak (to-faktorautentisering) som bidrar til å hindre uautorisert innsyn i konfidensielle opplysninger i systemer i skolesektoren hvor det lagres visse typer opplysninger om elever. Det er imidlertid mulig å omgå disse for flere av systemene som er i bruk i skolesektoren. Det er pågående prosesser for å utbedre sikkerhetshullene, men på revisjonstidspunktet var ikke disse ferdigstilte.

Når det gjelder skolenes praksis for å hindre uautorisert innsyn i konfidensielle opplysninger i skolesektoren, viser svarene i spørreundersøkelsene at det er en til dels vesentlig risiko for brudd på konfidensialiteten i skolesektoren; om lag én av fem svarer 21 % at de enten har delt passordet sitt med

[123] Stillingen var på revisjonstidspunktet ikke besatt, men kommunen viser til at de har leid inn ekstern hjelp med relevant kompetanse fra januar 2019 for å arbeide på dette feltet.

IT-avdelingen eller andre, noe som bryter med grunnleggende informasjonssikkerhetsprinsipper. Svarene i spørreundersøkelsen viser videre at det både forekommer at dokumenter med personopplysninger eller annen fortrolig informasjon blir oppbevart i ulåste skuffer eller hyller, at denne typen papirdokument oppbevares lett tilgjengelig, og at ansatte tar med seg konfidensielle papirdokument hjem. Også slik praksis utgjør vesentlig risiko for brudd på konfidensialiteten.

Bergen kommune har etablert noen rutiner og retningslinjer for **lagring av konfidensielle opplysninger**. Noen av retningslinjene ser imidlertid ikke ut til å være en integrert del av i kommunens styringssystem for personvern og informasjonssikkerhet, og det kommer frem av undersøkelsen at de heller ikke er kjente for sentrale ansatte når det gjelder systemsikkerhet i skolesektoren. Det er ikke tilfredsstillende at det som eksisterer av utfyllende retningslinjer knyttet til sikker lagring av konfidensielle opplysninger verken er kjent eller inngår i styringssystemet for informasjonssikkerhet. Dette gir økt sannsynlighet for feil og slik også risiko for at konfidensiell informasjon lagres uten tilstrekkelig sikring.

Revisjonen vurderer ellers at det i skolesektoren bare delvis er etablert rutiner og praksis for sikring av konfidensialitet med hensyn til bruk av sikker sone for lagring av konfidensielle opplysninger.

Bergen kommune har prosedyrer, rutiner og retningslinjer som stiller krav til **kryptering av konfidensielle opplysninger**. Både i oppdragsbeskrivelser, sjekklister og mer detaljert veiledningsmateriell går det frem hvilke typer opplysninger og informasjon som skal krypteres. Funn i undersøkelsen tyder imidlertid på det i skolesektoren bare delvis er en etablert praksis å kryptere konfidensielle opplysninger.

Tilgangsstyring

Kommunens styringssystem for personvern og informasjonssikkerhet plasserer ansvaret og de overordne oppgavene for å hindre uautorisert tilgang til informasjonssystemene. Det er i tilhørende dokument også nedfelt noen overordnede rutiner, regler og instrukser for å hindre uautorisert tilgang til informasjonssystemene.

Funn i undersøkelsen tyder på at det i de større systemene eid av skolesektoren er relativt lav risiko for at uautoriserte får tilgang, mens risikoen for dette er høyere i de mindre, pedagogiske systemene.

De gjennomførte sikkerhetstestene av kommunens IKT-systemer og fagsystemet *itslearning* avdekket ingen kritiske sårbarheter. Det ble imidlertid identifisert sårbarheter med både høy, moderat og lav risiko. Disse medfører risiko for brudd på informasjonssikkerheten i informasjonssystemene som blir benyttet i skolesektoren.

Kommunens system og rutiner for tilgangsstyring er ellers bare i noen grad egnet til sikre at ansatte får tilgangene de trenger når de trenger dem, og for å sikre at ansatte som slutter i kommunen mister tilgangene sine. Funn i undersøkelsen tyder på at det er en viss risiko for at ansatte ikke har tilganger de trenger, og en noe større risiko for at ansatte har tilganger de ikke har tjenstlig behov for.

Undersøkelsen viser også at praksis knyttet til vurdering av riktige tilganger ikke er tilstrekkelig innarbeidet i organisasjonen; nesten én av fire rektorer som deltok i spørreundersøkelsen svarer at det ikke er, eller at de ikke vet om det er, praksis knyttet til jevnlig vurdering av riktige tilganger. Dette er ikke tilfredsstillende all den tid det er rektorene som er ansvarlige for å melde videre behovet for endringer i tilgangene til informasjonssystemene.

For noen av de større systemene er det mulig å få oversikt over hvilke brukere som logger seg på. Det fremgår ikke i undersøkelsen om denne muligheten benyttes systematisk i skolenes informasjonssikkerhetsarbeid. Det er ikke mulig å loggføre brukte tilganger i de mindre systemene, noe som gjør at det ikke er mulig å avdekke eventuelle uautorisert tilganger i disse systemene. Skolesektoren i Bergen kommune har slik ikke tilstrekkelig oversikt over hvem som behandler informasjon i informasjonssystemene.

Opplæring og kompetanse

Bergen kommune har lagt til rette for at ansatte kan tilegne seg kunnskap og kompetanse knyttet til informasjonssikkerhet og personvern, gjennom blant annet plassering av opplæringsansvar og

tilgjengeliggjøring av veiledningsmateriell. Svarene i spørreundersøkelsen indikerer imidlertid at en relativt stor del av rektorene bare delvis oppgir å ha besørget nødvendig opplæring for sine ansatte knyttet til informasjonssikkerhet. Dette reflekteres i svar fra ansatte i skolesektoren på spørsmål om mottatt opplæring, der over halvparten av respondentene oppgir å ikke ha fått tilstrekkelig opplæring knyttet til personvern og informasjonssikkerhet.

Revisjonen er oppmerksom på at gjeldende styringssystem for informasjonssikkerhet relativt nylig ble utarbeidet og implementert, og videre at det er planer om å tilby de ansatte ytterligere opplæring. Likevel er det revisjonen sin vurdering at kommunen ikke fullt ut er i samsvar med krav og anbefalinger om å sikre tilstrekkelig informasjonssikkerhetskompetanse blant de ansatte i skolesektoren gjennom opplæringstiltak. Dette medfører økt sannsynlighet for at de ansatte i skolesektoren ikke har tilstrekkelig kompetanse innen informasjonssikkerhet, noe som øker risikoen for brudd på regelverket som gjelder for behandling av personopplysninger og for informasjonssikkerhet generelt. Funnene i undersøkelsen knyttet til informasjonssikkerhetskompetanse og –praksis tyder videre på at denne risikoen har gjort seg gjeldende i skolesektoren.

Med bakgrunn i funnene i denne forvaltningsrevisjonen anbefaler revisjonen at Bergen kommune gjennomfører tiltak for å sikre følgende:

1) at kommunens styringssystem for informasjonssikkerhet og personvern etterleves i skolesektoren, herunder at:
    a) roller og ansvar for informasjonssikkerhet og personvern tydeliggjøres og etterleves
    b) sentrale aktiviteter i styringssystemet praktiseres som forutsatt, inkludert at:
        i. det gjennomføres tilstrekkelige risikoanalyser
        ii. meldte avvik behandles og følges opp i samsvar med kommunens prosedyrer og rutiner
        iii. oversikt over personopplysninger som behandles i skolene er fullstendig og ajourført
2) at ansvar og rutiner for å hindre uautorisert innsyn i konfidensielle opplysninger tydeliggjøres og etterleves, inkludert bruk av sikker sone ved lagring av konfidensielle opplysninger og kryptering av konfidensielle opplysninger
3) at ansvar og rutiner for å hindre uautorisert tilgang til informasjonssystemene tydeliggjøres og etterleves, herunder sikre at ansatte har nødvendige tilganger, og ikke har tilganger uten at det foreligger et tjenstlig behov
4) at identifiserte tekniske risikoer i kommunens informasjonssystemer reduseres
5) at systemeiere, systemkoordinatorer, resultatenhetsledere og eventuelt andre med ansvar knyttet til informasjonssikkerhet og personvern i skolesektoren mottar tilstrekkelig opplæring og har nødvendige støtteverktøy for å kunne gjennomføre sine respektive informasjonssikkerhetsoppgaver
6) at de ansatte mottar tilstrekkelig opplæring innen informasjonssikkerhet, og at de vet hvor de kan finne oppdaterte rutiner og retningslinjer for informasjonssikkerhet

Vedlegg 1: Høringsuttalelse

BERGEN KOMMUNE

Byrådsavdeling for barnehage, skole og idrett

Deloitte AS
Frode Løvlie
PhD | Manager | Risk Advisory
Lars Hilles gate 30,
5008 Bergen, Norway

Høringssvar

Vår referanse: 2019/102139-1
Saksbehandler: Jan Eide
Dato: 29. november 2019

Unntatt offentlighet: **Offl § 5**

Høringsuttalelse - Rapport om forvaltningsrevisjon av informasjonssikkerhet i skolesektoren i Bergen kommune

Byrådsavdeling for barnehage, skole og idrett har mottatt rapportutkast om forvaltningsrevisjon av informasjonssikkerhet i skolesektoren på høring. Byrådsavdelingen har gått gjennom rapportutkastet, og finner at det fremstår som grundig og informativt. Vi har opplevd prosessen knyttet til revisjonen som god i de fleste faser av arbeidet. Selv om vi ikke deler revisors oppfatninger på alle punkter, ser vi at vi kan ha stor nytte av rapporten i det pågående arbeidet med å videreutvikle byrådsavdelingens systemer og praksis innen informasjonssikkerhet inklusive på personvernområdet. Som rapporten viser, har byrådsavdelingen allerede iverksatt flere tiltak for å legge til rette for en god informasjonssikkerhet, samtidig som det er forbedringspotensialer på flere områder.

Som det også fremkommer i rapporten, har det oppstått enkelte personvernrelaterte avvik i forbindelse med implementering av nytt oppvekstadministrativt system, Vigilo. Byrådsavdelingen tar disse hendelsene svært alvorlig. Vi har fullt fokus på å følge opp avvikene, og adressere rotårsakene til hendelsene for å unngå at tilsvarende skal skje i fremtiden. Samtidig er det viktig at byrådsavdelingen fortsetter det viktige arbeidet med å legge til rette for trygge og effektive kommunikasjonsløsninger med publikum.

På enkelte områder ser vi i denne høringsuttalelsen behov for å kommentere revisors observasjoner og vurderinger særskilt. Det er en omfattende rapport som i stor grad fokuserer på overordnede utfordringer knyttet til områder som ledelse og styring, internkontroll, og roller og ansvar. Samtidig har revisor begrenset datainnhenting via intervju til å intervjue fire personer som alle i all hovedsak arbeider med informasjonssikkerhet. I tillegg ble enkelte, konkrete problemstillinger avsjekket per telefon med seksjonssjef for HR, digitalisering og virksomhetsstyring i etterkant av den ordinære intervjurunden. Revisor har imidlertid ikke gjennomført et helhetlig intervju med verken kommunaldirektør for byrådsavdelingen, seksjonssjef for HR, digitalisering og virksomhetshetsstyring eller med andre representanter for ledelsen. Dette gjør at rapporten fremstår som mangelfull når det gjelder hvordan ledelsen arbeider strategisk for å sikre en tilfredsstillende informasjonssikkerhet, og om planer for videreutvikling av dette arbeidet fremover.

Byrådsavdelingen hadde i forkant av revisjonen sett behov for å gjøre organisatoriske endringer, hvor en viktig målsetting blant annet har vært å styrke arbeidet med informasjonssikkerhet. Det har vært gjennomført en grundig kartlegging av ulike organisatoriske modeller, for å legge til rette for tilfredsstillende styring og kontroll, samt effektiv kommunikasjon mellom ulike nivåer i byrådsavdelingen. Resultatet av arbeidet er at byrådsavdelingen ble omorganisert med virkning fra 1. juli 2019, og det ble etablert en seksjon med et dedikert ansvar for å følge opp arbeidet med informasjonssikkerhet. Revisor nevner omorganiseringen i rapporten, men vi mener det legges for lite vekt på dette viktige organisatoriske grepet som ble tatt blant annet for å styrke arbeidet med informasjonssikkerhet i avdelingen. Videre virker det forvirrende at revisor ikke skiller tydelig mellom ny og gammel organisasjonsmodell i rapporten.

Ledelsen har iverksatt en rekke tiltak for å styrke byrådsavdelingens arbeid med informasjonssikkerhet. I tillegg til overnevnte organisatoriske grep har det i hele 2019 vært engasjert en medarbeider med spisskompetanse innen informasjonssikkerhet, som har arbeidet fulltid med dette temaet. Vedkommende har fylt stillingen som informasjonssikkerhetsmedarbeider etter denne ble opprettet sommeren 2019, i tillegg til at det har blitt leid inn ekstra spisskompetanse på området ved behov. Av rapporten fremstår det imidlertid som om den aktuelle stillingen ikke har vært besatt, hvilket gir et misvisende bilde av status og av byrådsavdelingens satsing på dette området. Byrådsavdelingen har også inngått et tettere samarbeid med Seksjon for digitalisering og innovasjon sentralt i Bergen kommune, og det er etablert en arbeidsgruppe på tvers av enhetene for å styrke arbeidet med informasjonssikkerhet. Det er gjort endringer i styringen av prosjektet som skal implementere det oppvekstadministrative systemet Vigilo, det arbeides aktivt med kartlegging av arbeidsprosesser for slik å identifisere etablerte kontroller og risiko knyttet til informasjonssikkerhet, og med ROS-analyser for å sikre at det foreligger helhetlige og oppdaterte risikovurderinger, og at nødvendige tiltak etableres i en handlingsplan og følges opp.

Flere steder i rapporten fremgår det at områdelederne i byrådsavdelingen ikke har formelle fullmakter når det gjelder å følge opp informasjonssikkerhet. Av fagfullmakten til områdelederne før omorganiseringen fremgikk det imidlertid at de skal "se til at skoler, barnehage og PPS gir tjenester i henhold til gjeldende lov- og regelverk, vedtatte økonomiske rammer og øvrige kommunale styringsdokumenter og føringer". Dette innebærer et helhetlig ansvar, også for informasjonssikkerhet. Vi anerkjenner imidlertid at resultatene av intervju og spørreundersøkelse som revisor har gjennomført indikerer at det er behov for å iverksette tiltak for å tydeliggjøre dette ansvaret.

Vi ser også behov for å kommentere revisors nettfiskeforsøk. Her mener vi det er problematisk å trekke for bastante konklusjoner ut fra testen som er gjennomført i Bergen kommune. For at undersøkelsen skulle kunne la seg gjennomføre, måtte Bergen kommune fjerne sine vanlige sikkerhetsmekanismer, og stanse de normale rutinene og prosessene som kommunen har rundt håndtering av slike informasjonssikkerhetshendelser. I vurderingen av undersøkelsens funn bør dette vektlegges. Vi anerkjenner imidlertid at det er viktig og nødvendig å arbeide med informasjonssikkerhetskulturen i byrådsavdelingen. Dette er en grunnleggende forutsetning for å oppnå en tilfredsstillende informasjonssikkerhet. Rapporten er således et nyttig verktøy når det gjelder å sikre tilstrekkelig fokus på dette temaet.

Revisor har anbefalt at det iverksettes syv tiltak som en oppfølging av forvaltningsrevisjonen. De fleste av anbefalingene er relatert til opplæring for å sikre at kommunens medarbeidere er kjent med rutiner og krav knyttet til informasjonssikkerhet, samt til tiltak for å sikre etterlevelse av interne krav. I tillegg omhandler en anbefaling tekniske risikoer i kommunens informasjonssystemer. Vi er enig i at det er behov for å iverksette tiltak i henhold til revisors anbefalinger. I vårt arbeid med kontinuerlig forbedring og videreutvikling av informasjonssikkerhetsarbeidet i byrådsavdelingen, vil vi gå nøye gå gjennom revisors øvrige observasjoner og vurderinger, og vurdere hvilke ytterligere tiltak som bør iverksettes. Det er allerede startet et arbeid med å etablere en helhetlig oversikt over tiltak for å styrke informasjonssikkerheten i byrådsavdelingen, hvor det vektlegges en tydelig plassering av ansvar for oppfølging av hvert enkelt tiltak, samt fastsettelse av frist for gjennomføring.

Et av områdene vi vil ha fokus på i tiden fremover, er å styrke sikkerhetskulturen i byrådsavdelingen. Dette vil vi blant annet gjøre ved å kommunisere krav og viktigheten av å etterleve disse, samt ved å følge opp etterlevelse tettere for slik å legge til rette for en mer enhetlig og trygg praksis innen informasjonssikkerhet. Vi vil også vektlegge økt grad av samarbeid på tvers av etater og seksjoner, for slik å legge til rette for en mer enhetlig kultur på tvers av byrådsavdelingen. Både seksjonssjef for HR, digitalisering og virksomhetsstyring

og kommunaldirektør vil følge opp dette arbeidet tett, for å sikre effektiv iverksettelse av nødvendige tiltak.

Arbeidet med personvern og informasjonssikkerhet vil også styrkes gjennom strategi for informasjonssikkerhet som Byrådsavdeling for finans, næring og eiendom vil legge frem for byrådet i løpet av våren.

Med hilsen
Byrådsavdeling for barnehage, skole og idrett

Linn Kristin Engø
Byråd

Vedlegg 2: Kommentar til høringsuttalen

Under vil revisjonen kommentere et par momenter i kommunens høringsuttale.

Kommunen skriver i høringsuttalen at det at revisjonen ikke har gjennomført intervjuer med ledelsen i byrådsavdelingen gjør at rapporten fremstår som mangelfull når det gjelder hvordan ledelsen arbeider strategisk for å sikre en tilfredsstillende informasjonssikkerhet, og om planer for videreutvikling av dette arbeidet fremover. Til dette vil revisjonen først bemerke at formålet med forvaltningsrevisjonen var å se på hvordan informasjonssikkerheten faktisk er ivaretatt i skolesektoren, ikke hvordan det skal bli ivaretatt. Videre gjennomførte revisjonen – delvis parallelt med denne forvaltningsrevisjonen – en forvaltningsrevisjon av overordnet informasjonssikkerhet i Bergen kommune, og hadde slik allerede informasjon om hvordan ansvar og roller er fordelt på området, samt om hvordan styringen av informasjonssikkerhet på overordnet nivå er organisert. Revisjonen vil også bemerke at valg av intervjuobjekter ble gjort i samråd med kommunen, samt at det verken i verifiseringen eller i høringen har kommet frem informasjon som tilsier at vi har manglet vesentlig informasjon.

Når det gjelder områdeledernes formelle fullmakter på informasjonssikkerhetsområdet, hadde revisjonen allerede justert teksten for å reflektere dette etter at kommunen i forbindelse med verifiseringen informerte om at slike fullmakter foreligger. Vi har nå gjort ytterligere justeringer for å tydeliggjøre dette.

Når det gjelder stillingen som informasjonssikkerhetsansvarlige som på revisjonstidspunktet ikke var besatt, har revisjonen justert teksten slik at det nå går fram at kommunen har leid inn ekstern hjelp med relevant kompetanse fra januar 2019 for å arbeide på dette feltet.

Hva gjelder kommunens kommentarer knyttet til nettfiskeforsøket og våre konklusjoner, vil revisjonen bemerke at vi allerede har omtalt både formålet med testen (om *ansatte* i skolen praktiserer trygg e-postbruk) og forutsetningene for gjennomføringen (inkludert at kommunen måtte slå av sine tekniske og organisatoriske sikkerhetsmekanismer) i avsnitt 6.2.3. Vi har derfor ikke gjort justeringer knyttet til dette.

Vedlegg 3: Revisjonskriterier

Informasjonssikkerhet

Informasjonssikkerhet handler om sikring av informasjon med hensyn til *konfidensialitet*, *integritet* og *tilgjengelighet*.

Å sørge for *konfidensialitet* innebærer å hindre ikke-autorisert innsyn i informasjon som ikke skal være tilgjengelig for alle; å sørge for *integritet* innebærer å hindre ikke-autorisert endring og sletting av informasjon; å sørge for tilgjengelighet innebærer å sikre tilgang til informasjon ved behov for tilgang.

Krav i lov og forskrift

Regelverket knyttet til informasjonssikkerhet omfatter blant annet personopplysningsloven.[124] Denne trådde i kraft 20. juli 2018, og gjennomfører EU sin personvernforordning – kjent som GDPR[125] – i norsk lov.

Artikkel 4 i personvernforordningen definerer begrepene brukt i forordningen i 26 punkt. Under er noen relevante punkt presentert:

> 1) «personopplysninger» enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet,
>
> 2) «behandling» enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring
>
> …
>
> 7) «behandlingsansvarlig» en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes …
>
> 8) «databehandler» en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige
>
> …
>
> 12) «brudd på personopplysningssikkerheten» et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet

I kommunen er det byråden som er behandlingsansvarlig.[126] Databehandlere er eventuelle tjenesteleverandører til kommunen som behandler personopplysninger, som for eksempel leverandør av lønn- og personalsystem. Forordningen artikkel 28 nr. 3 stiller krav om at behandling av personopplysninger utført av en databehandler skal være underlagt en avtale med nærmere spesifisert innhold (bokstav a til h).

Internkontroll og styringssystem for informasjonssikkerhet

Artikkel 24 og 28 i forordningen omhandler den behandlingsansvarlige og databehandleren sitt ansvar for å etablere internkontroll; nr. 1 i artikkel 24 sier blant annet at den behandlingsansvarlige skal «gjennomføre

[124] Lov om behandling av personopplysninger (personopplysningsloven)
[125] General Data Protection Regulation.
[126] Jf. *En veiledning om internkontroll og informasjonssikkerhet* (Datatilsynet 2009, s. 11).

egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov», mens artikkel 28 nr. 1 stiller krav om at databehandlere skal gi tilstrekkelig med garantier «for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordningen og vern av den registrertes rettigheter.»

Personvernforordningen artikkel 32 nr. 1 stiller videre krav om informasjonssikkerhet ved behandling av personopplysninger. Kravene som stilles er at informasjonssikkerheten skal være tilfredsstillende med hensyn til personopplysningene sin konfidensialitet, integritet, tilgjengelighet og robusthet gjennom at det blir satt i verk egnede tekniske og organisatoriske tiltak basert på risikovurderinger. Artikkelen inneholder regler som omhandler hva risikovurderingene skal legge vekt på.

I tillegg til reglene i personvernforordningen knyttet til internkontroll og informasjonssikkerhet, er kommunen gjennom eForvaltningsforskriften § 15 forpliktet til å ha et internkontrollsystem basert på anerkjente standarder for styringssystem for informasjonssikkerhet:

> Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.
>
> Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.

Direktorat for forvaltning og IKT (Difi) er pekt ut som ansvarlig for å gi anbefaling knyttet til hvilket styringssystem for informasjonssikkerhet som bør benyttes. Difi anbefaler at offentlige virksomheter baserer seg på ISO/IEC 27001:2013, som er en internasjonal standard for styringssystem for informasjonssikkerhet.

Kapittel 5.3 i ISO275001 stiller som krav at den «øverste ledelsen skal sikre at ansvar og myndighet for roller som er relevante for informasjonssikkerheten, er tildelt og kommunisert.» Videre blir det stilt krav om at:

> Den øverste ledelsen skal tildele ansvar og myndighet for:
>
> a) å sikre at ledelsessystemet for informasjonssikkerhet oppfyller kravene i denne internasjonale standarden, og
> b) å rapportere til øverste ledelse om prestasjonen til ledelsessystemet for informasjonssikkerhet.

Punktene A.6.1.1 og A.6.1.2 i ISO275001 sin liste over sikringsmål og –tiltak, omhandler roller og ansvar, og er gjengitt i tabellen under:

A.6.1.1	Roller og ansvar for informasjonssikkerhet	*Sikringstiltak* Alt ansvar for informasjonssikkerhet skal være definert og tilordnet
A.6.1.2	Arbeidsdeling	*Sikringstiltak* Oppgaver og ansvar innenfor ulike områder skal være segregert for å redusere mulighetene for uautorisert eller utilsiktet modifisering eller misbruk av organisasjonens aktiva.

Ytterligere krav i personvernforordningen

Personvernforordningen stiller krav om kommunen skal informere registrerte personer om at den behandler personopplysninger om dem, jf. artikkel 12-14. Artikkel 12 nr. 1 pålegger kommunen at slik informasjon skal være «kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk.» Datatilsynet skriver i sitt veiledningsmateriell at en behandlingsansvarlig for eksempel kan etterkomme deler av informasjonskravene ved å ha en personvernerklæring.

Personvernforordningen pålegger kommunen å utpeke et personvernombud, jf. artikkel 37 bokstav a. Artikkel 38 regulerer stillingsvilkårene for personvernombudet, og det går blant annet fram der at kommunen skal sikre at personvernombudet blir involvert i rett tid i alle spørsmål som gjelder personopplysninger (nr. 1), at kommunen skal stille tilstrekkelig ressurser til rådighet for at personvernombudet kan gjennomføre oppgavene pålagt stillingen i personvernforordningen artikkel 38 (nr. 2), at personvernombudet skal være uavhengig og rapportere direkte til byråden (nr. 3), og at personvernombudet er bundet av taushetsplikt (nr. 5).

Personvernombudet sine lovpålagte oppgaver går fram av artikkel 39. Her går det fram at personvernombudet blant annet skal kontrollere at personvernforordningen blir overholdt (bokstav b), gi råd om vurdering av personvernkonsekvenser (bokstav c), og samarbeide med Datatilsynet (bokstav d).

Forordningen stiller videre nye og skjerpede krav til hva avvik som skal meldes til Datatilsynet. Hovedregelen slik denne går fram i artikkel 33 er at alle avvik som skyldes brudd på personopplysningssikkerheten (utilsikta sletting, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet, jf. artikkel 4 punkt 12), skal meldes til Datatilsynet innen 72 timer. Artikkel 33 nr. 3 stiller krav hva avviksmeldingene skal inneholde. Artikkel 34 stiller nærmere krav om hva vilkår som må være oppfylt for at kommunen ikke skal melde ifra om personopplysningssikkerhetsbruddet til den eller de registrerte som avviket gjelder. Jf. artikkel 33 punkt 5, skal kommunen dokumentere alle avvik, og hvilke tiltak som er satt i verk.

Artikkel 30 nr. 1 i personvernforordningen stiller krav om at kommunen skal føre en protokoll over behandlingsaktivitetene av personopplysninger som blir utført. forordningen stiller nærmere krav til innholdet i denne protokollen, som for eksempel navn og kontaktopplysning på den behandlingsansvarlige (bokstav a), formålet med behandlingen (bokstav b), en beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger (bokstav c). Nr. 3 i artikkelen stiller krav om at protokollen skal være skriftlig og nr. 4 sier at protokollen skal gjøres tilgjengelig for Datatilsynet dersom de ber om det.

Forordningen stiller i tillegg krav om at det i noen situasjoner skal gjøres risikovurderinger av behandlingen av personopplysninger. I artikkel 35 nr. 1, står det at:

> Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for vernet av personopplysninger.

Dette er et krav om at kommunen skal gjennomføre en vurdering av personvernkonsekvensene av behandling av personopplysninger der slik behandling medfører høy risiko for rettigheter og friheter for fysiske personer. Jf. artikkel 39 om personvernombudet sine oppgaver, skal vedkommende gi råd om vurdering av personvernkonsekvenser og kontrollere gjennomføringen av denne dersom kommunen ber om det.

Kompetanse

Som nevnt er kommunen gjennom eForvaltningsforskriften § 15 forpliktet til å ha en internkontroll basert på anerkjente standarder for styringssystem for informasjonssikkerhet. Departementet har utpekt direktorat for forvaltning og IKT (Difi) som ansvarlig for å gi anbefalinger knyttet til hvilket styringssystem for informasjonssikkerhet som bør benyttes, og Difi anbefaler at offentlige virksomheter baserer seg på ISO/IEC 27001:2013. Kapittel 7.2 i standarden sier at kommunen skal:

> e) fastslå hvilken kompetanse som er nødvendig for personen(e) som utfører arbeid under organisasjonens styring, og som påvirker dens informasjonssikkerhetsprestasjon;
> f) sikre at disse personene har kompetanse tilegnet gjennom passende utdanning, opplæring eller erfaring;
> g) der det er relevant, treffe tiltak for å erverve nødvendig kompetanse og evaluere virkningen av tiltakene som er truffet; og
> h) oppbevare relevant dokumentert informasjon som bevis på kompetanse.

I merknaden til punkt 7.2, står det at «Aktuelle tiltak kan for eksempel omfatte å sørge for opplæring, veiledning eller omplassering av nåværende ansatte eller innleie av eller kontraktinngåelse med kompetente personer.»

I Datatilsynet sin veileder *Internkontroll og informasjonssikkerhet*[127] omhandler blant annet oppfølging og opplæring. Her går det fram at målet med brukeropplæring er å sikre at brukerne er oppmerksomme på trusler mot personvernet og informasjonssikkerheten generelt, og at de er gitt anledning til å etterleve dette i sitt daglige arbeid. Opplæringen bør være tilpasset de ulike målgruppene sitt behov for opplæring og fordeles over tid. Brukarene bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystem for å redusere potensielle risikoer.

I tillegg til anbefalingen om opplæring av ansatte som følger av ISO-standarden, kan man utlede et krav om opplæring og kjennskap til system, rutiner og regelverk blant ansatte fra kommuneloven § 20 nr. 2 andre ledd, som sier at byråden «skal sørge for at administrasjonen drives i samsvar med lover, forskrifter og overordnede instrukser, og at den er gjenstand for betryggende kontroll.» Et sentralt tiltak i ethvert internkontrollsystem vil være at det er på plass tilstrekkelig opplæring til at de ansatte er i stand til å gjennomføre sine arbeidsoppgaver i samsvar med lover, krav og forventninger.

Annet regelverk

I tillegg til kravene i personvernforordningen og eForvaltningsforskriften er det også flere andre regler knyttet til informasjonssikkerhet som er relevant for kommunen. Kravene i disse regelverkene er i noen grad overlappende med kravene til et styringssystem for informasjonssikkerhet.

I helseregisterloven er det gitt konkrete føringer knyttet til behandlingen av helseopplysninger, og her kommer det blant annet fram konkrete krav knyttet til informasjonssikkerhet (§ 16). Det er utarbeidet en norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren (Norma), som stiller krav med utgangspunkt i både personopplysningsforskriften og helseregisterloven. I Norma er det også innarbeidet ulike krav knyttet til taushetsplikt og informasjonsrett etter særlovgiving for kommunehelsetjenester, sosialtjenester, psykisk helsevern, samt forvaltnings- og offentlighetslov.

Kommunen er også omfattet av sikkerhetsloven, og har som følge av dette plikt til å ha forsvarlig informasjonssikkerhet for informasjon som kan være kritisk for å forhindre trusler som spionasje, sabotasje og terrorhandlinger. Disse kravene kan være relevante for kommunen for eksempel når det gjelder å beskytte vannforsyningen fra forurensing av drikkevann.

Kommunale vedtak

I forvaltningsrevisjonsrapporten fra 2015, anbefalte revisjonen at kommunen gjennomførte følgende tiltak knyttet til styringssystem for informasjonssikkerhet:

1. Utbedre de elementene i styringssystemet hvor det er påpekt mangler, med særlig vekt på
   risikovurderinger
   sikkerhetsrevisjoner
   avvikshåndtering
   ledelsens gjennomgang
Sørge for at systemeiere har tilstrekkelig opplæring og støtteverktøyer for å kunne gjennomføre sine oppgaver.
Sørge for at retningslinjer og rutiner på informasjonssikkerhet er oppdatert og sikre at alle ansatte kjenner til hvor man finner rutinene.
4. Ved utarbeidelse av ny strategi for informasjonssikkerhet, fastsette krav til oppfølging av og rapportering på gjennomføring av tiltak, samt eventuell rullering av planer og tiltak.

Bystyret vedtok i møte 12. mai 2015 å be Byrådet om å følge opp de forslag til tiltak som fremgikk av rapporten.

[127] *Internkontroll og informasjonssikkerhet.* Datatilsynet. Publisert 23.06.2018. https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/

Vedlegg 4: Sentrale dokumenter og litteratur

Lov og forskrift

- Justis- og beredskapsdepartementet: Lov om behandling av personopplysninger (personopplysningsloven). LOV-2018-06-15-38.
- Justis- og beredskapsdepartementet: Forskrift om behandling av personopplysninger (personopplysningsforskriften). FOR-2018-06-15-876.
- Kommunal- og moderniseringsdepartementet: Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften). FOR-2004-06-25-988.

Forarbeider, rundskriv, veiledere mv.

- Diverse veiledningsmateriell fra Datatilsynet
- Diverse veiledningsmateriell fra Direktorat for forvaltning og IKT (Difi)
- ISO/IEC 27001:2013

Dokumenter fra kommunen

- Overordnet rutine for håndtering av avvik som gjelder personvern og informasjonssikkerhet.
- Avslutning av arbeidsforhold. Sjekkliste for leder
- Databehandleravtaler meldt inn til personvernombud
- Dokumentasjon på gjennomførte ROS og DPIA
- Verktøy for vurdering av personvernkonsekvens
- Protokoll over behandlingsaktiviteter
- Reglement for akseptabel bruk av IKT
- Retningslinjer for IT-sikkerhet. Bergen kommune. 2002.
- Styrende dokument for digitalisering og IKT i Bergen kommune. Organisering, roller og ansvar
- Agenda og samskrivingsnotat fra IKT-kontaktmøte 2016, 2017 og 2018.
- Referat fra IKT-driftsmøte (juni og september 2017 og oktober 2018)
- Presentasjon fra autorisasjonskurs i Extens. Bergen kommune.
- Diverse interne rutiner systemkoordinatorer (Eksamensberedskap (PAS), nytt skoleår og sammenligne personer (Extens))
- Overordnet passordinstruks. Bergen kommune.
- Diverse e-post og intern korrespondanse.
- Diverse dokument og oversikter fra Bergen kommunes intranett, BK prosjekt og BK kvalitet.
- Diverse dokumenter og korrespondanse knyttet til informasjonssikkerhetsbruddet i Vigilo
- Styringssystem for personvern og informasjonssikkerhet
    - Reglement for trygg digitalisering
    - Veileder for trygg digitalisering
    - Veileder personvern og informasjonssikkerhet for ledere
    - Oppdrag – personvern og informasjonssikkerhet for kommunaldirektør
    - Oppdrag – personvern og informasjonssikkerhet for resultatenhetsledere
    - Oppdrag – personvern og informasjonssikkerhet for systemeiere
    - Oppdrag – personvern og informasjonssikkerhet for leder av EDD
    - Oppdrag for alle ansatte for akseptabel bruk av IKT
    - Mandat for informasjonssikkerhetsforum
    - Mandat for personvernombud
    - Vurdering av personvernkonsekvenser for avvik

Vedlegg 5: Nettfiskeforsøk

Innhold

1.0 Innledning

Som del av forvaltningsrevisjon av informasjonssikkerhet i Bergen kommune har Deloitte gjennomført en Phishing Awareness Test (nettfiskeforsøk) blant ansatte i Bergen kommune.

Denne rapporten dokumenterer resultatet av testen.

2.0 Formål

Phishingangrep mot ulike typer virksomheter forekommer i stadig større grad, og gjennomføres av både cyber-kriminelle med begrensede midler, men også av statlige aktører i forbindelse med mer målrettede angrep. Formålet med disse angrepene kan være å tilegne seg sensitiv informasjon fra brukere, eller installere ondsinnet programvare.

I Norge har man den senere tiden sett flere større virksomheter, både offentlig og privat, bli utsatt for phishing-angrep der formålet har vært å installere såkalt *ransomware* på brukernes datamaskiner. *Ransomware* er en spesialisert form for ondsinnet programvare som krypterer filer i det lokale filsystemet og som krever en løsesum for å låse filene opp igjen.

Deloitte har i forbindelse med forvaltningsrevisjon av informasjonssikkerhet i Bergen kommune gjennomført et phishingangrep mot ansatte i Bergen kommune. Formålet er å teste om de ansatte praktiserer trygg e-postbruk, og vise hvorvidt de er oppmerksomme på sikkerhetsrisikoen som er forbundet med e-post-bruk. I tillegg bidrar phishingangrepet til praktisk læring og bevisstgjøring blant de ansatte om egen e-postbruk.

Resultatene fra phishing-testen gir et øyeblikksbilde av de ansattes aktuelle eksponering for phishingangrep. Det danner også et referansepunkt (benchmark) som kan brukes for å måle effekten av tiltak som etableres etter at testen er gjennomført.

3.0 Konklusjon

Av de totalt 13 365 ansatte i Bergen Kommune som ble utsatt for phishingangrepet klikket 3 226 (24,14 %) av mottakerne på lenken og besøkte den eksterne hjemmesiden som var opprettet i forbindelse med angrepet. 2 213 (16,56 %) valgte deretter å oppgi sitt brukernavn og passord på en ukjent hjemmeside uten sikker forbindelse (HTTPS).

Phishing Awareness Testen mot ansatte i Bergen Kommune viser manglende oppmerksomhet om risikoer knyttet til phishingangrep hos en betydelig gruppe ansatte. Merk at den gjennomførte testen regnes å være av middels kompleksitet, og dermed skal være mulig å avsløre som et phishingangrep. Det er vår konklusjon at risikoen for at en ekstern angriper kan få tilgang til eksempelvis medarbeidernes e-post og andre interne systemer som benytter samme e-post og passord, er stor.

Deloitte har gjennomført en rekke lignende Phishing Awareness Tester, med samme kompleksitet og formål, for andre virksomhet. Resultatene fra disse testene viser at det gjennomsnittlig er 22,73 % av mottakerne som klikker på lenken i phishing e-posten, og 18,60 % som deretter oppgir sitt brukernavn og passord. Resultatet for Bergen Kommune viser et middels modenhetsnivå sett i forhold til et gjennomsnitt fra tidligere Phishing Awareness Tests gjennomført av Deloitte.

Vi gjør oppmerksom på at den gjennomførte testen kun er et øyeblikksbilde av modenhet og bevissthet knyttet til phishingangrep i Bergen kommune. Den utførte testen er designet ut fra dagens trusselbilde, og det blir forløpende utviklet nye angrepsmetoder. Det er en tendens til at angrep i økende grad målrettes virksomheter og individer, og det anbefales derfor at det jevnlig gjennomføres Phishing Awareness Test for å kartlegge medarbeidernes modenhet når det gjelder typen angrep.

Under følger en rekke anbefalinger som kan bidra til å styrke de ansattes bevissthet om phishingangrep.

4.0 Anbefalinger

Deloitte anbefaler at det iverksettes målrettede tiltak til å styrke bevisstheten om phishingangrep blant ansatte i Bergen kommune. Tiltak bør fokusere på faren ved å taste inn personlige opplysninger på eksterne og ukjente hjemmesider, og på hjemmesider uten en sikker forbindelse (HTTPS), ettersom resultatene fra testen viser at ansatte ikke er tilstrekkelig bevisste disse risikoene.

Det er videre viktig at policyer og retningslinjer på IT-sikkerhetsområdet blir kommunisert ut i virksomheten, og at disse oppdateres fortløpende ut fra det til enhver tids gjeldende trusselbilde. Det er også viktig at kommunen har en beredskapsplan som sikrer rask handling ved reelle angrep, da testen viser at de fleste medarbeidere klikket på lenken innen den første timen etter utsendelse. Bergen kommune bør i tillegg vurdere å gjennomføre kurs i brukerbevissthet, der de ansatte blir trent i å identifisere phishing-e-post og rapportere om mistenkelige henvendelser.

For å redusere risikoen for phishingangrep mer generelt anbefaler vi følgende tiltak:

- **Medarbeideropplysning.** Sørge for at medarbeiderne er klar over risikoen som er forbundet med å åpne e-post fra ukjente avsendere, og sørge for at de er mer kritiske når det gjelder hvilke hjemmesider de besøker, og hvilke data det er greit å avgi og laste ned.

- **Løpende testing av medarbeiderne**. Gjennomføre løpende testing av medarbeidernes bevissthet rundt phishingangrep. Dette vil bidra til å styrke ansattes bevissthet, og gjøre det mulig å følge opp hvorvidt de tiltakene som er implementert har effekt.

- **Passe på maskerte lenker**. Undersøk lenker i e-post ved å holde musen over lenken, og se hvilken adresse denne peker på.

- **Benytte et effektivt spamfilter**. Spamfilteret vil ikke kunne stoppe mer målrettede phishingangrep, men vil kunne hindre åpenbare angrep før disse når brukeren. *Blacklisting* av kjente phishing-URL'er vil forhindre at medarbeiderne mottar disse.

- Sørge for at det foreligger en **rutine for hvordan et phishing-angrep mot virksomheten håndteres,** herunder hva som meldes ut til brukerne, og hvordan dette gjøres.

- Sørge for å holde infrastruktur og klienter, inkludert nettlesere og plug-ins, oppdatert til **nyeste versjon**. Hvis brukerne blir lurt til å besøke sider som kan infisere maskinene deres, vil dette redusere risikoen for at de blir kompromittert.

- Sørge for å ha et **oppdatert antivirusprogram** på alle klienter og servere. Oppdaterte antivirusprogram vil redusere risikoen for at en skadelig kode sprer seg til andre maskiner, dersom den angriper en maskin via et phishingangrep.

- **Begrense brukernes tilganger** basert på tjenstlig behov.

- Benytte **2-faktorautentisering** ved innlogging på eksternt tilgjengelige applikasjoner.

Les mer om forsvarsmekanismer mot phishing her: https://www.owasp.org/index.php/Phishing

For beskrivelse av phishingangrepet og resultater se 5.0 Vedlegg 1.

5.0 Vedlegg 1: Gjennomgang av resultater

I forbindelse med forvaltningsrevisjon av informasjonssikkerhet i Bergen kommune har Deloitte gjennomført en Phishing Awareness Test (nettfiskeforsøk) blant ansatte i Bergen Kommune.

5.1 Omfang og avgrensning

Phishing Awareness Testen gikk ut på at en konstruert phishing e-post ble sendt ut til alle medarbeidere, med hensikt å lokke de ansatte til å taste inn sensitive opplysninger på en usikker hjemmeside.

Testen var designet som en invitasjon til en fiktiv undersøkelse - «Etikkundersøkelse 2019». I invitasjonen ble de ansatte oppfordret til å klikke på en lenke, og deretter å taste inn deres brukernavn og passord for å delta i etikkundersøkelsen. Et angrep er ansett som vellykket når medarbeideren har tastet inn brukernavn og passord.

Målgruppen for testen var fast ansatte i Bergen kommune. Ansatte som jobber i kommunalt AS, er politikere, har en stillingsprosent under 40 %, er ekstrahjelper, vikarer, o.l., eller har en av stillingstypene assistenter, renholdere, studenter og pensjonister, ble utelukket fra forsøket. På bakgrunn av dette mottok Deloitte en liste med e-postadressene til 13 365 ansatte i Bergen Kommune. Disse mottok phishing-e-posten 15. mai i tidsrommet kl. 12.00-18.00.

«Etikkundersøkelsen» var aktiv fra onsdag 15. mai kl. 12:00 til onsdag den 22. mai kl. 12:00.

Beskrivelse av testen

Testen besto av en e-post på norsk med invitasjon til en etikkundersøkelse, og en tilhørende hjemmeside på norsk. Formålet med testdesignet som ble benyttet var å få medarbeideren til å tro at det ble gjennomført en etikkundersøkelse i Bergen kommune, der det ble stilt krav om innloggingsdetaljer for å besvare undersøkelsen.

Phishingangrepet ble utformet slik at det skulle fremstå som troverdig, bl.a. ved å inneholde kommunens logo og omhandle et tema som angår de fleste ansatte i kommunen. E-posten inneholdt imidlertid også elementer som gjorde det mulig for mottagerne å avsløre testen. E-posten hadde «Dcure Global» og adressen «etik@dcure.dk» som avsender, som ikke er relatert til Bergen kommune. Den inneholdt også en lenke som pekte på et domene som heller ikke var relatert til Bergen kommune.

Figur 1 (under) viser eksempel på e-posten som de ansatte mottok.


on 22-05-2019 14:17

Dcure Global <etik@dcure.dk>

Etikkundersøkelsen 2019

To

Kjære kollega,

Du er en av de utvalgte til å motta etikkundersøkelsen 2019. Grunnet ny personvernlovgivning er Bergen kommune underlagt nye krav til etikk.

I den forbindelse ber vi om at du bruker ca. 3 minutter til å besvare spørsmål knyttet til etikk, holdninger og adferd.

Dine svar vil behandles fortrolig. Undersøkelsen gjennomføres av DCure Global Benchmarking Group, og du får tilgang via følgende link:

Klikk her for å svare på undersøkelsen

På forhånd takk for deltakelsen.

Vi ber om at du svarer på undersøkelsen innen 22. mai 2019.

BERGEN
KOMMUNE

Figur 1: *Phishing-e-post med invitasjon til «Etikkundersøkelsen 2019».*

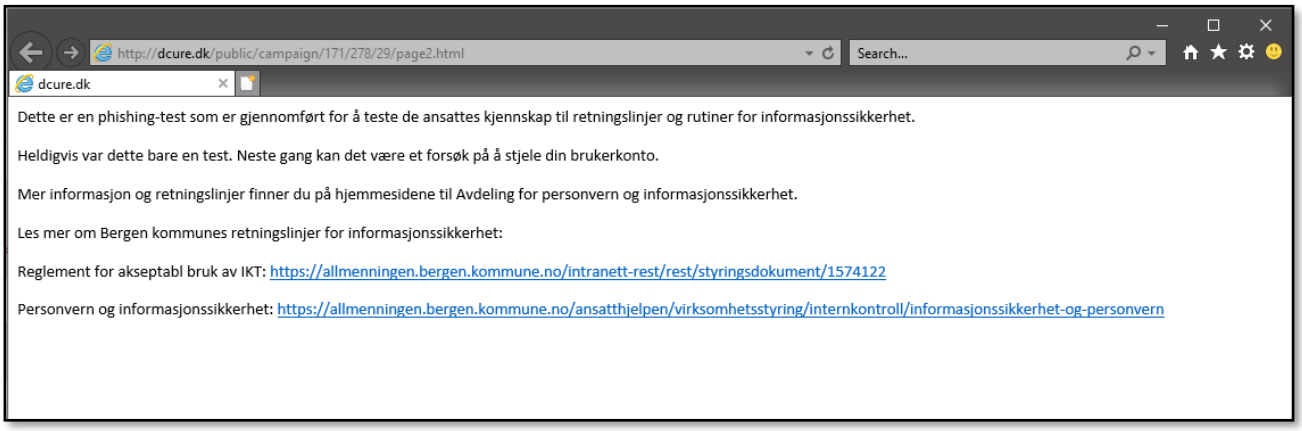
I e-posten ble de ansatte oppfordret til å klikke på en lenke for å besvare undersøkelsen. Lenken bestod av en unik URL generert for hver medarbeider, som gjør det mulig å spore hver enkelt medarbeiders besøk på nettsiden lenken førte til.

Ved å klikke på lenken i e-posten ble medarbeideren rutet til hjemmesiden <http://dcure.dk> der de ble bedt om å taste inn sitt brukernavn og passord for å svare på selve undersøkelsen (se figur 2).[1]

Figur 2: *«Etikkundersøkelsen 2019» – hjemmeside*

[1] Merk at nettsiden <http://dcure.dk> ikke lenger er aktiv da testen er avsluttet.

Ansatte som tastet inn brukernavn og passord på nettsiden kom videre til en nettside («landing page») der de ble informert om at de hadde blitt utsatt for et phishingangrep, og som lenket til rutiner og retningslinjer for informasjonssikkerhet i Bergen kommune (se figur 3).



Figur 3: *«Etikkundersøkelsen 2019»-landing page etter at brukernavn og passord er tastet inn.*

Merknad

Vi vil gjøre oppmerksom på at vi bevisst har unnlatt å benytte HTTPS på våre phishing-nettsider, da dette som regel ikke brukes i reelle phishingangrep. HTTPS brukes til å kryptere trafikk som er sendt mellom bruker og webserver, og mangel på dette betyr at trafikken i stedet blir sendt ukryptert.

Av personvernhensyn har ikke Deloitte tatt vare på ev. brukernavn og passord som er tastet inn på den falske nettsiden. Å sende brukernavn og passord til vår server ville gjort det mulig å verifisere hvorvidt de ansatte oppga riktige passord i forbindelse med phishing-testen, men dette ville også medført en sikkerhetsrisiko for at brukernavn og passord kan komme på avveie.

De brukernavn og passord som de ansatte har tastet inn på phishing-nettsiden er derfor ikke blitt lagret hos Deloitte.

5.2 Analyseresultat

DMARC-analyse

Deloitte har analysert de mottakerdomener som er benyttet i testen for å undersøke om det benyttes Domain-based Message Authentication, Reporting and Conformance (DMARC).

DMARC er en sikkerhetsstandard for e-post som er designet til å avdekke og forhindre e-post med forfalsket avsender i å nå frem til mottakerne. Såfremt DMARC understøttes, vil dette være en hjelp mot phishingangrep, da det assisterer tekniske foranstaltninger med å verifisere hvorvidt det er snakk om en forfalsket e-post eller ikke, i tillegg til at det gir mulighet til å registrere hvorvidt det er skjedd forfalskning av ens domene.

Domene	Understøtter DMARC
bergen.kommune.no	**Nei**

Tabell 1: *DMARC understøttelse*

Resultat av Phishing Awareness Test - «Etikkundersøkelsen 2019»

Det ble i forbindelse med den utførte Phishing Awareness Testen utsendt e-post til 13 365 ansatte i Bergen Kommune.

Samlet sett klikket 3 226 av medarbeiderne på lenken i e-posten og besøkte dermed hjemmesiden til «Etikkundersøkelsen», en ukjent hjemmeside med en usikker forbindelse. Det tilsvarer 24,14 % av det totale antallet mottakere. Deretter var det 2 213 som tastet inn brukernavn og passord på nettsiden. Av de som besøkte

hjemmesiden oppga dermed 68,60 % brukernavn og passord. Dette tilsvarer 16,56 % av alle mottakerne som mottok phishing-e-posten.

Testen viser at de fleste medarbeidere klikket på lenken innen den første timen etter utsendelse.

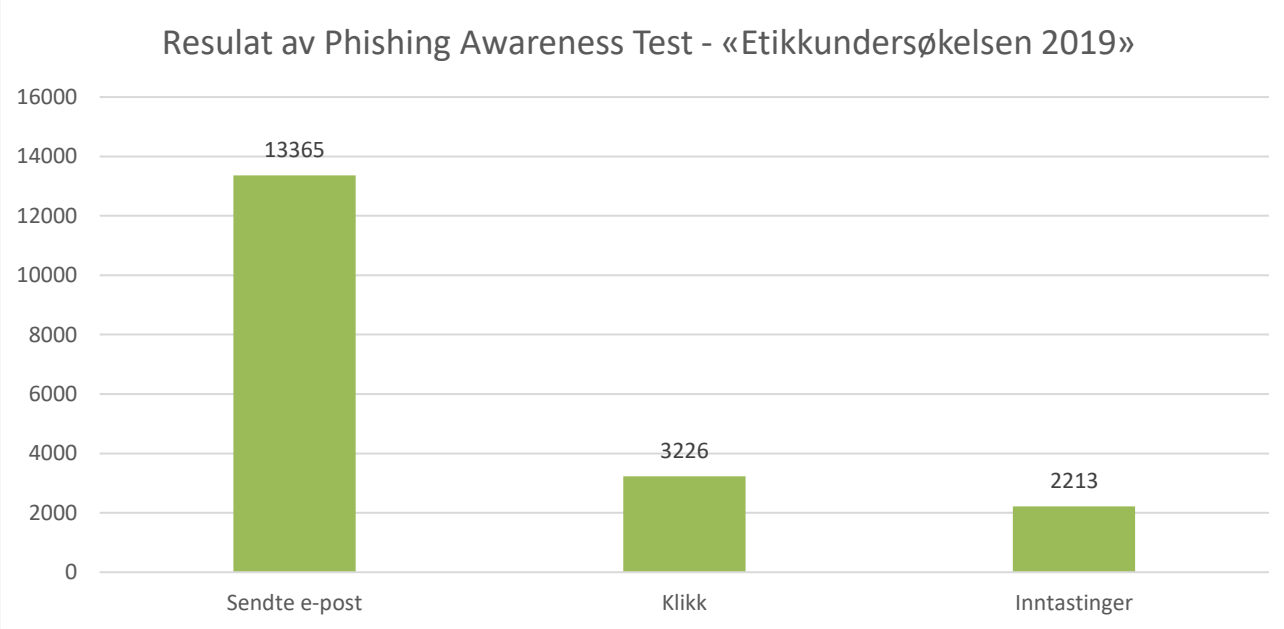
Utbyttet av det samlede angrepet bestod dermed av 2 213 passord med tilhørende e-post, noe som utgjør en **høy IT-sikkerhetsrisiko**.

Tabellen under gir oversikt over vellykkede phishingangrep under den utførte phishing-testen.

Test	Dato	Antall mottakere	Antall klikk på lenke	Antall inntastede brukernavn og passord
Etikkundersøkelsen 2019	15.05.2016	13 365	3 226 (24,14 %)	2 213 (16,56 %)

Tabell 2: *Resultatoversikt*

Figur 4 nedenfor viser det overordnede resultatet av phishingangrepet.



Figur 4: *Resultat av Etikkundersøkelsen 2019*

Som det fremgår av figur 4, ble det utsendt 13 365 phishing-e-post. 3 226 (24,14 %) medarbeidere klikket på lenken i e-posten, og 2 213 (16,56 %) av disse oppga brukernavn og passord.

5.3 Metoder, verktøy m.m.

En Phishing Awareness Test er én av flere metoder for å vurdere virksomheters modenhet innen Cyber Security. Tabellen viser hvilke tester som kan gjennomføres, og hvilken test som er gjennomført og analysert i denne rapporten.

Test-type	Intern sikkerhets-analyse	Ekstern sikkerhets-analyse	Web-applikasjons-test	Penetratsjons-test	WIFI test	Firewall Audit	Phishing Awareness Test
Utført	-	-	-	-	-	-	✓

Metode, verktøy og kompetanse

Deloitte anvender en rekke verktøy basert på industristandarder og egenutviklede programmer. Disse verktøyene holdes løpende oppdatert for å sikre at de nyeste uregelmessigheter detekteres.

Alle detekterte uregelmessigheter samles i vår kunnskapsdatabase, hvor de analyseres og behandles. Alle uregel-messigheter i følgebrevet er verifisert manuelt som foreskrevet i kunnskapsdatabasens manuelle verifiserings-tilgang.

Den påfølgende QA-prosessen (Quality Assurance) foretas av våre høyt kvalifiserte IT-sikkerhetskonsulenter, som sikrer at rapportene oppnår høyeste kvalitet.

Metoder

Ved Deloittes sårbarhetsanalyser og Phishing Awareness Test anvendes følgende metoder:

Host Discovery-analyse

- Blottlegning av nettverkskomponenter
- Identifisering av IP-adresser på aktivt utstyr samt åpne porter/tjenester
- Blottlegning av webservere
- Scanning av webadresser samt blottlegning av sidens struktur, inkl. antall filer og filstørrelser
- Utvidet Host Discovery-analyse inneholder dessuten detaljer om enhetene og webserverne
- Delta-rapportering
- Avrapportering med teknisk rapport.

Intern sikkerhetsanalyse og ekstern sikkerhetsanalyse

- Test for elementære angrep og/eller målrettede angrep, evt. med insiderkunnskap og brukeradgang
- Kontroll av falske positiver ved manuell verifisering (Deloittes kunnskapsdatabase)
- Analyse av resultater
- Avrapportering med følgebrev og detaljert teknisk rapport.

Webapplikasjonstest

- Test for elementære angrep og/eller målrettede angrep, evt. med insiderkunnskap og brukeradgang
- Kontroll av falske positiver ved manuell verifisering (Deloittes kunnskapsdatabase)
- Analyse av resultater
- Avrapportering med følgebrev og detaljert teknisk rapport.

WIFI-test

- Test av Access Points og lokalisering av uautoriserte Access Points
- Test for elementære angrep og/eller målrettede angrep, evt. med insiderkunnskap og brukeradgang
- Test av kryptert WI-FI, log-in, brute force på kryptering
- Analyse av resultater
- Avrapportering med følgebrev.

Penetrasjonstest

- Kreative tester med egen og/eller nyutviklede verktøy til det spesifikke system
- Test for elementære angrep og/eller målrettede angrep, evt. med insiderkunnskap og brukeradgang
- Kontroll av falske positiver ved manuell verifisering (Deloittes kunnskapsdatabase)
- Analyse av resultater
- Avrapportering med følgebrev og detaljert teknisk rapport.

Firewall Audit

- Analyse av brannmurens konfigurasjon
- Gjennomgang av regelsettet for identifisering av uregelmessigheter såsom overlappende regler, for brede regler, inaktive regler osv.
- Vurdering av sikkerheten i brannmuren basert på operativsystemet
- Analyse av resultater
- Avrapportering med følgebrev og detaljert teknisk rapport.

Phishing Awareness Test

- Analyse av medarbeidernes awareness mht. phishingangrep
- Analyse av SPF record-oppsetninger
- Gjennomgang av personsensitive opplysninger som er offentlig tilgengelige på websiden
- Analyse av resultater
- Avrapportering med følgebrev og detaljert teknisk rapport.

Verktøy

Deloittes verktøykasse utvides og oppdateres hele tiden med anerkjente de facto-IT-sårbarhetsstandardverktøy. Dette suppleres med egenutviklede scanning- og verifiseringsverktøy.

Videre anvendes diverse andre hacker- og open source-verktøy, hvor vi har hatt adgang til å gjennomgå verktøyets kildekode.

Kompetanse

Deloittes IT-sikkerhetskonsulenter blir løpende utdannet på internasjonale kurs og workshops, og besitter en rekke anerkjente sertifiseringer. Mange har derfor spisskompetanse innen ulike deler av IT-sikkerhetsområdet.

Vedlegg 6: Sikkerhetstest av IKT-systemet

Vedlegget er unntatt offentlighet etter offentlighetsloven § 24 tredje ledd.

Vedlegg 7: Sikkerhetstest av *itslearning*

Vedlegget er unntatt offentlighet etter offentlighetsloven § 24 tredje ledd.

Deloitte.