Deloitte.

Forvaltningsrevisjon | Bergen kommune

Informasjonssikkerhet

September 2019

«Forvaltningsrevisjon av informasjonssikkerhet»

September 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 kommunen. Formålet med forvaltningsrevisjonen har vært å undersøke i hvilken grad kommunens styringssystem for informasjonssikkerhet etterleves. Forvaltningsrevisjonen er en oppfølging av tilsvarende forvaltningsrevisjoner gjennomført i 2009 og 2014.

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

Tilfredsstillende informasjonssikkerhet

Bergen kommune har et oppdatert styringssystem for personvern og informasjonssikkerhet. Det er ikke avdekket funn i undersøkelsen som tyder på at dette ikke er i samsvar med kravene i gjeldende regelverk. Kommunen har gjennom styringssystemet etablert prosedyrer, retningslinjer og systemer som er egnet til å utbedre flere av svakhetene påpekt i revisjonen fra 2015. Samtidig registrerer revisjonen at praksis på flere av de samme områdene fortsatt har forbedringspotensial.

Kommunen har prosedyre for melding av avvik som er i samsvar med regelverket, og system som legger til rette for melding av avvik. Tilsendt avviksstatistikk og svar i spørreundersøkelsen tyder imidlertid på at kommunens avvikspraksis ikke fullt ut samsvarer med relevante anbefalinger eller generelle prinsipper for god internkontroll. Revisjonen mener at kommunen bare delvis har fulgt opp anbefaling nr. 1c fra 2015.

Kommunen har også etablert verktøy og retningslinjer for gjennomføring av risikovurderinger, og gjennomfører slike. Selv om kommunen har gjort fremskritt på dette området siden 2015, er flere av risikovurderingene mangelfulle, og flere systemer mangler risikovurderinger. Revisjonen mener derfor kommunen bare delvis har fulgt opp anbefaling nr. 1a fra 2015.

I styringssystemet stilles det krav om gjennomføring av sikkerhetsrevisjoner. Det har blitt gjennomført slike, og etter planen skal det gjennomføres flere. Omfanget av sikkerhetsrevisjoner er imidlertid lavt, og på grunn av manglende og mangelfulle risikovurderinger, har ikke kommunen grunnlag for å velge ut de områdene og systemene for sikkerhetsrevisjon der risikoen for brudd på informasjonssikkerheten er størst. Revisjonen mener kommunen bare delvis har fulgt opp anbefaling nr. 1b fra 2015.

Styringssystemet stiller krav til og inneholder prosedyrer for gjennomføring av ledelsens gjennomgang. Gjennom reetableringen av informasjonssikkerhetsforum høsten 2018 er de organisatoriske forutsetningene for å kunne gjennomføre ledelsens gjennomgang på plass, og ledelsens gjennomgang ble også gjennomført for 2018. Revisjonen mener kommunen langt på vei har fulgt opp anbefaling nr. 1d fra 2015.

Kommunen har en informasjonssikkerhetsstrategi, men denne er ikke styrende for informasjonssikkerhetsarbeidet i kommunen. Kommunen har plan om å rullere eller ev. utarbeide ny informasjonssikkerhetsstrategi, og derigjennom følge opp anbefaling nr. 4 fra 2015.

Tilgangsstyring

Bergen kommune har system og rutiner for tilgangsstyring. Disse vurderes å bare i noen grad være egnet til å sikre at ansatte i kommunen får tilgangene de trenger, og for å sikre at ansatte som slutter i kommunen mister tilgangene sine. Kommunens rutine og praksis knyttet til tilgangsstyring ved skifte av arbeidssted i kommunen vurderes som sårbar, både på grunn av organisatoriske og tekniske forhold.

De gjennomførte sikkerhetstestene avdekket ingen kritiske sårbarheter i kommunens eksterne eller interne nett. Det ble imidlertid identifisert sårbarheter med både høy, moderat og lav risiko. Disse medfører risiko for brudd på informasjonssikkerheten i kommunens informasjonssystemer.

Etterlevelse av utvalgte lovkrav

Bergen kommune har etablert system og praksis for melding om behandling av personopplysninger og utarbeidelse av protokoller med oversikt over slike behandlinger, og har også utarbeidet slike protokoller. Disse er imidlertid i ulik grad av ferdigstillelse, og kommunen har ikke fullstendig oversikt over alle

systemene der det muligens behandles personopplysninger. Manglende fullstendighet i oversikt og protokoller gjør at kommunen ikke fullt ut oppfyller relevante krav i personvernforordningen.

Kommunen har retningslinjer, rutiner og verktøy for vurdering av personvernkonsekvenser, og det kommer ikke frem indikasjoner på at disse bryter med krav i regelverket. Kommunen har gjennomført noen vurderinger av personvernkonsekvenser. Manglende risikovurderinger kombinert med mangelfull oversikt over hvilke personopplysninger som behandles betyr imidlertid at kommunen ikke har full oversikt over hvilke personopplysninger som behandles med høy risiko, og derfor heller ikke har tilstrekkelig kunnskapsgrunnlag for å gjennomføre vurdering av personvernkonsekvenser ved behandling av personopplysninger med høy risiko, jf. krav i personvernforordningen.

Kommunen har et personvernombud. Det kommer ikke frem indikasjoner på at mandatet til stillingen ikke oppfyller krav i personvernforordningen. Bergen kommune har også en personvernerklæring, og heller ikke her er det indikasjoner på at denne ikke er i samsvar med krav i personvernforordningen.

Helhetlige føringer

Styringssystemet for personvern og informasjonssikkerhet med tilhørende dokumenter gir felles føringer for informasjonssikkerhet, og det er slik lagt til rette for en oppdatert og helhetlig tilnærming til informasjonssikkerhet i kommunen. Kommunen oppfyller slik første del av anbefaling nr. 3 fra 2015 om å «sørge for at retningslinjer og rutiner på informasjonssikkerhet er oppdatert».

Respondentene i spørreundersøkelsen er i relativt liten grad kjent med hvor de finner relevante rutiner og retningslinjer, og i enda mindre grad har de lest og gjort seg kjent med obligatoriske og sentrale styrende dokumenter. Revisjonen mener derfor det bør iverksettes tiltak for å sikre at styringssystemet faktisk blir etterlevd.

Oppgaver og ansvar

Ansvar og oppgaver knyttet til informasjonssikkerhet fremgår i kommunens styringssystem. Konsernansvaret for informasjonssikkerhet er tydelig lagt til BFIE, og det foreligger fullmakter og avtaler som plasserer ansvar og oppgaver nedover i byrådsavdelingen. Det fremgår videre hvilket ansvar som påhviler ulike roller, samt hvilke oppgaver disse skal utføre for å sikre god informasjonssikkerhet; blant annet er både ansvaret og de respektive oppgavene til resultatenhetsledere, systemeiere og ansatte skriftliggjort.

Funn i undersøkelsen tyder imidlertid på at verken systemeierne eller resultatenhetslederne i tilstrekkelig grad er sitt informasjonssikkerhetsansvar bevisst. Sett i sammenheng med funn knyttet til respondentenes kjennskap til og etterlevelse av kommunens regelverk, rutiner, veiledere, prosedyrer mm. for informasjonssikkerhet (se under), mener revisjonen at Bergen kommune ikke i tilstrekkelig grad har tydeliggjort ansvar og oppgaver knyttet til informasjonssikkerhet.

Funn i undersøkelsen tyder òg på at kommunen ikke i tilstrekkelig grad har sørget for at «systemeiere har tilstrekkelig opplæring og støtteverktøyer for å kunne gjennomføre sine oppgaver», og slik ikke fulgt opp anbefaling nr. 2 fra 2015.

Revisjonen registrerer at blant annet kommunens størrelsen og den parlamentariske styringsmodellen i kommunen fremholdes som medvirkende årsaker til at det kan være utfordrende for BFIE å fullt ut sikre at de enkelte byrådsavdelinger ivaretar sitt ansvar for informasjonssikkerhet. Revisjonen vil understreke viktigheten av at den enkelte byrådsavdeling i kommunen følger opp sitt ansvar for å etterleve kommunens styringssystem for personvern og informasjonssikkerhet, for eksempel ved å sikre at deres representant i informasjonssikkerhetsforum har tilstrekkelig myndighet.

Opplæring, kompetanse og praksis

Bergen kommune har lagt til rette for at ansatte kan tilegne seg kunnskap og kompetanse knyttet til informasjonssikkerhet og personvern gjennom blant annet obligatoriske kurs og veiledningsmateriell. Svarene i spørreundersøkelsen indikerer imidlertid at en relativt stor del av resultatenhetslederne bare delvis oppgir å ha besørget nødvendig opplæring for sine ansatte knyttet til informasjonssikkerhet. Dette reflekteres i svar 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 det er relativt kort tid siden styringssystemet ble etablert, men vil likevel påpeke at Bergen kommune ikke oppfyller krav og anbefalinger om å sikre tilstrekkelig informasjons-sikkerhetskompetanse blant de ansatte gjennom opplæringstiltak. Dette understøttes av funn i undersøkelsen som viser at ikke alle ansatte i Bergen kommune har tilstrekkelig kjennskap til retningslinjer og rutiner for informasjonssikkerhet, at ansatte i Bergen kommune ikke i tilstrekkelig grad etterlever retningslinjer og rutiner for informasjonssikkerhet, samt at informasjonssikkerhetspraksisen blant ansatte bryter med flere grunnleggende informasjonssikkerhetsprinsipp. Revisjonen mener derfor kommunen ikke har fulgt opp andre del av anbefaling nr. 3 fra 2015 om å «sikre at alle ansatte kjenner til hvor man finner rutinene».

Revisjonen sine anbefalinger fremgår i kapittel 6.

Innhold

1.	Innledning	10
2.	Om tjenesteområdet	13
3.	Tilfredsstillende informasjonssikkerhet	14
4.	Oppgaver og ansvar	32
5.	Kompetanse blant de ansatte	45
6.	Konklusjon og anbefalinger	61
Vedlegg 1 : Høringsuttalelse		64
Vedlegg 2 : Revisjonskriterier		66
Vedlegg 3 : Sentrale dokumenter og litteratur		70
Vedlegg 4 : Nettfiskeforsøk		72
Vedlegg 5 : Sikkerhetstester		82

Detaljert innholdsfortegnelse

1. Innledning 10
   - 1.1 Bakgrunn 10
   - 1.2 Formål og problemstillinger 10
   - 1.3 Avgrensning 10
   - 1.4 Metode 11
   - 1.5 Revisjonskriterier 12

2. Om tjenesteområdet 13
   - 2.1 Organisering 13

3. Tilfredsstillende informasjonssikkerhet 14
   - 3.1 Problemstilling 14
   - 3.2 Revisjonskriterier 14
   - 3.3 Rutiner og retningslinjer for informasjonssikkerhet 15
   - 3.4 Helhetlige føringer for informasjonssikkerhet 28

4. Oppgaver og ansvar 32
   - 4.1 Problemstilling 32
   - 4.2 Revisjonskriterier 32
   - 4.3 Ansvar og oppgaver knyttet til informasjonssikkerhet 33
   - 4.4 Vurdering 43

5. Kompetanse blant de ansatte 45
   - 5.1 Problemstilling 45
   - 5.2 Revisjonskriterier 45
   - 5.3 Kjennskap til retningslinjer og rutiner for informasjonssikkerhet blant ansatte 45
   - 5.4 Vurdering 58

6. Konklusjon og anbefalinger 61
   - Tilfredsstillende informasjonssikkerhet 61
   - Oppgaver og ansvar 62
   - Opplæring, kompetanse og praksis 62

Vedlegg 1 : Høringsuttalelse 64

Vedlegg 2 : Revisjonskriterier 66

Vedlegg 3 : Sentrale dokumenter og litteratur 70

Vedlegg 4 : Nettfiskeforsøk 72

Vedlegg 5 : Sikkerhetstester 82

Figurer

Figur 1: Organisasjonskart for BFIE 13

Figur 2: Hierarkisk oppbygging av styringssystemet for informasjonssikkerhet og personvern 15

Figur 3: Modell for trygg digitalisering 29

Figur 4: Informasjonssikkerhet og personvern på Allmenningen 30

Figur 5: Tydelig informasjonssikkerhetsansvar for resultatenhetsleder 37

Figur 6: Kjennskap til sentrale dokument (resultatenhetsledere) 38

Figur 7: Utfyllende retningslinjer for informasjonssikkerhet 38

Figur 8: Resultatenhetsleder: dokumentert oversikt over behandling av informasjon 39

Figur 9: Dokumentasjon og systematiske risikovurderinger 39

Figur 10: Vet du hvem som er systemeiere av systemene som benyttes i din resultatenhet? 42

Figur 11: Stillingens informasjonssikkerhetsansvar (N=314) 42

Figur 12: Besørget opplæring 46

Figur 13: Mottatt opplæring 47

Figur 14: Informasjon om informasjonssikkerhetspraksis 48

Figur 15: Behandling av personopplysninger 48

Figur 16: Lest kommunens IKT-reglement 49

Figur 17: Husker IKT-reglementet 49

Figur 18: Kjennskap til sentrale dokument (alle) 50

Figur 19: Tilfredsstillende skriftlige retningslinjer for informasjonssikkerhet 51

Figur 20: Viktigheten av informasjonssikkerhet 52

Figur 21: Fokus på informasjonssikkerhet 52

Figur 22: Kontakt ved spørsmål om informasjonssikkerhet og personvern 53

Figur 23: Hvem skal du kontakte dersom du har spørsmål knyttet til informasjonssikkerhet? (N=211) 53

Figur 24: Delt passord 54

Figur 25: Hva gjør du vanligvis når du i løpet av arbeidsdagen forlater PC-en du bruker? 54

Figur 26: Møterompraksis o.l. 55

Figur 27: Oppbevaring av dokumenter med personopplysninger eller annen fortrolig informasjon 55

Figur 28: Meldte avvik (N=76) 56

Figur 29: Tydelige retningslinjer for bruk av e-post 57

Figur 30: Resultater nettfiskeforsøk per byrådsavdeling 58

Tabeller

Tabell 1: Svarprosent per byrådsavdeling 11

Tabell 2: Sikkerhetsmål for personvern og informasjonssikkerhet 15

Tabell 3: Internt ansvar for melding av avvik 18

Tabell 4: Avviksstatistikk informasjonssikkerhet (mars-august 2019) 19

Tabell 5: Akseptkriterier for overordnet ROS 20

Tabell 6: Risikovurdering 25

Tabell 7: Rangering av sårbarheter etter konsekvens 26

Tabell 8: Rangering av sårbarheter etter sannsynlighet 26

Tabell 9: Ansvar for informasjonssikkerhet i Bergen kommune 33

Tabell 10: Informasjonssikkerhetsroller 35

Tabell 11: Ansvar knyttet til systemeier- og systemkoordinatorrollen 40

Tabell 12: Oversikt over systemeiere 41

1. Innledning

1.1 Bakgrunn

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

I denne rapporten har revisjonen vurdert Bergen kommunes oppfølging av forvaltningsrevisjonsrapporten «Informasjonssikkerhet i Bergen kommune» fra 2015. Videre har vi undersøkt kommunens praksis for å ivareta informasjonssikkerheten, samt testet om de ansatte har kjennskap til og etterlever retningslinjer og rutiner for informasjonssikkerhet. I tillegg har revisjonen vurdert om kommunen etterlever et utvalg lovkrav i den nye personopplysingsloven som trådte i kraft i 2018.

Med bakgrunn i funnene i forvaltningsrevisjonen fra 2015, anbefalte revisjonen at Bergen kommune vurderte å gjennomføre følgende tiltak:

1) Utbedre de elementene i styringssystemet hvor det er påpekt mangler, med særlig vekt på
   a) risikovurderinger
   b) sikkerhetsrevisjoner
   c) avvikshåndtering
   d) ledelsens gjennomgang
2) Sørge for at systemeiere har tilstrekkelig opplæring og støtteverktøyer for å kunne gjennomføre sine oppgaver.
3) 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 rapportens forslag til tiltak.

1.2 Formål og problemstillinger

Formålet med forvaltningsrevisjonen har vært å undersøke i hvilken grad kommunens styringssystem for informasjonssikkerhet etterleves. Dette har vi gjort gjennom å følge opp forvaltningsrevisjonene av informasjonssikkerhet i Bergen kommune som ble gjennomført i 2009 og 2014, inkludert oppfølgingen gjort av kommunen per 01.09.2018 som rapportert 20.11.2018.[1]

Med bakgrunn i formålet har følgende problemstillinger blitt undersøkt:[2]

1. I hvilken grad er det etablert tiltak for å tilfredsstille krav i lovverket knyttet til informasjonssikkerhet?
   a. Er det innført rutiner og retningslinjer i samsvar med anbefalingene fra rapporten i 2015, og etterleves disse?
   b. I hvilken grad er det gitt føringer for å sikre en helhetlig tilnærming til informasjonssikkerhet i kommunen?
2. I hvilken grad er ansvar og oppgaver knyttet til informasjonssikkerhet tydeliggjort?
3. I hvilken grad har de ansatte 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 personopplysnings-sikkerheten kan få store konsekvenser, både for kommunen og enkeltmennesker. Gjennomgangen omfatter også informasjonssikkerhet knyttet til annen informasjon, som sensitive opplysninger og fortrolige opplysninger.

---

[1] Kontrollutvalget 20.11.2018 sak 75/18 byrådets rapportering jf. BEBY 51/18 status på funn og anbefalinger i vesentlige revisjoner de siste 3 år.
[2] For å sikre sammenlignbarhet, er problemstillingene likelydende med forvaltningsrevisjonen fra 2015.

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 til september 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.

1.4.2 Intervju

For å få supplerende informasjon til de skriftlige kildene, har Deloitte intervjuet fire personer som er involvert i arbeidet med og har et særskilt ansvar knyttet til informasjonssikkerhet; forhenværende konstituert personvernombud, direktør for seksjon for digitalisering og innovasjon konsern, kommunaldirektør for HR, digitalisering og eiendom og leder for enhet for digitale driftstjenester.

1.4.3 Spørreundersøkelse

Revisjonen har gjennomført en elektronisk spørreundersøkelse blant et strategis utvalg ansatte i Bergen kommune. Formålet med spørreundersøkelsen var å kartlegge kjennskap og holdning til informasjonssikkerhet blant de ansatte. Spørreundersøkelsen besto både av spørsmål som ble stilt i spørreundersøkelsene gjennomført i 2009 og 2014, og noen nye spørsmål.

Der vi har relevante tall å sammenligne med mellom 2009, 2014 og 2019, gjengir vi dette i rapporten. Det er likevel viktig å ta forbehold om at utvalgsmetoden i de tre undersøkelsene er noe ulik; i 2009 ble det gjennomført et begrenset utvalg basert på e-postlister fra ulike PPT-kontorer og skoler, mens respondentene i 2014 og 2019 ble valgt fra en oversikt over alle ansatte i Bergen kommune.[3]

Totalt ble 957 ansatte bedt om å svare på spørreundersøkelsen. Etter flere påminnelser kom det til slutt inn 384 svar. Dette gir en total responsrate på 40 %.

Tabell 1: Svarprosent per byrådsavdeling

Byrådsavdeling	Svarprosent
Byrådsavdeling for barnehage, skole og idrett	39 %
Byrådsavdeling for byutvikling	48 %
Byrådsavdeling for helse og omsorg	36 %
Byrådsavdeling for klima, kultur og næring	63 %
Byrådsavdeling for sosial, bolig og inkludering	46 %
Byrådsavdeling for finans, innovasjon og eiendom	45 %
Byrådsleders avdeling	48 %
Bystyrets organer	100 %
Totalt	**40 %**

1.4.4 Sikkerhetstester

Revisjonen har gjennomført sikkerhetstester i ulike deler av kommunens IKT-system. Formålet med testene har vært å undersøke om og hvordan kommunen i praksis ivaretar den tekniske informasjonssikkerheten. For å gjøre dette har revisjonen gjennomført forskjellige undersøkelser og tester for å

[3] 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.

kartlegge og identifisere eventuelle sårbarheter i IKT-systemene som ved utnyttelse svekker konfidensialiteten, integriteten og/eller tilgangen til kommunens infrastruktur og/eller data.

Sikkerhetstestene ble gjort både fra utsiden (internett) og innsiden (intranett) av kommunens nettverk. I testen fra utsiden 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.

Den interne sikkerhetstesten ble gjennomført via fjerntilgang til tre fysiske maskiner som stod i kommunens interne nettverk.[4] Fokuset for denne sikkerhetstesten var å avdekke hvorvidt eksisterende sikkerhets-kontroller og/eller filtreringsmekanismer (primært brannmur) 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.

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[5] eller tilsvarende destruktive tester.

Den tekniske rapporten etter sikkerhetstestene er å finne i vedlegg 5. Vedlegget er unntatt offentlighet etter offentlighetsloven § 24 tredje ledd.

1.4.5 Nettfiskeforsøk

For å teste i hvilken grad de ansatte har kjennskap til retningslinjer og rutiner for informasjonssikkerhet, har revisjonen gjennomført et nettfiskeforsøk.[6] Revisjonen har sendt offisielt-utseende men falske e-poster for å undersøke om og i hvilken grad ansatte 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.[7]

Rapporten fra nettfiskeforsøket er å finne i vedlegg 4.

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 kommunen for verifisering, og faktafeil er rettet opp i den endelige versjonen. Høringsutkast av rapporten er sendt til byråd for finans, innovasjon og eiendom for uttale. Byrådens høringsuttalelse er å finne i vedlegg 1.

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 forvaltningsrevisjon. I dette prosjektet er revisjonskriteriene i hovedsak hentet fra Lov om behandling av personopplysninger (personopplysningsloven). Kriteriene er nærmere presentert innledningsvis i hvert kapittel, og i vedlegg 2.

---

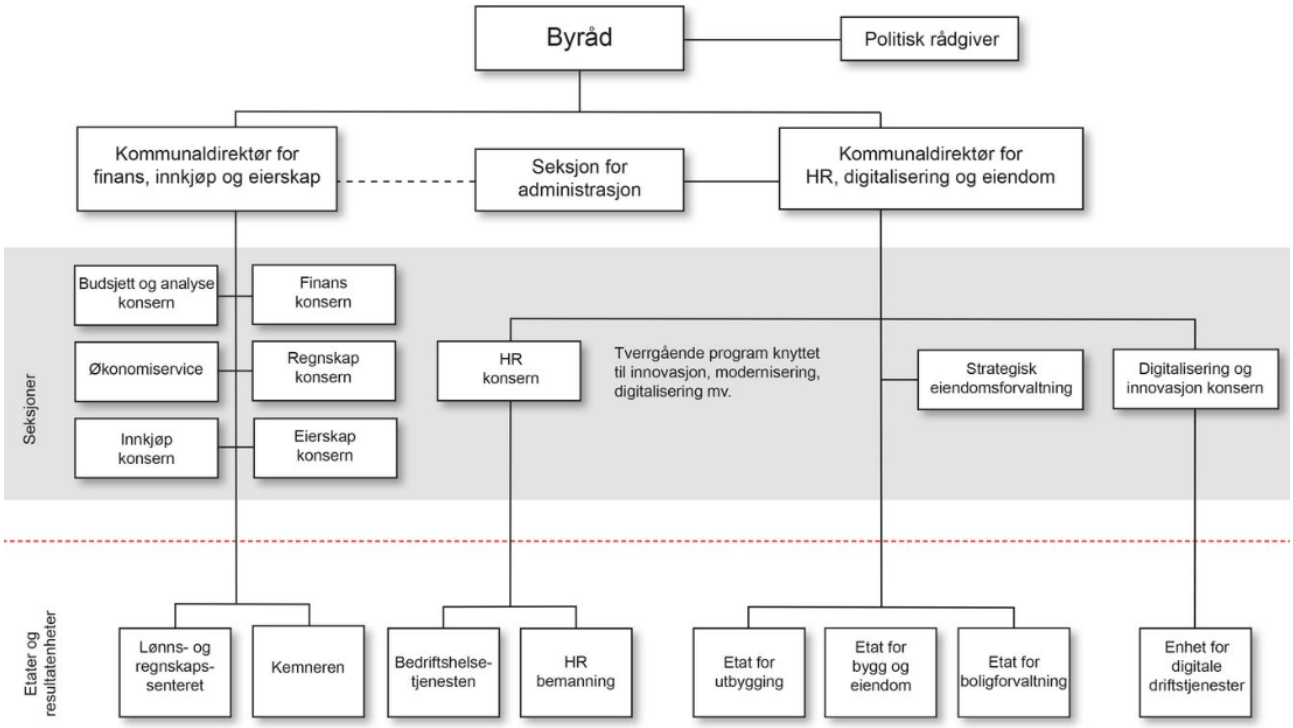
[4] Én av disse var konfigurert som en regulær PC for ansatte, én som en elev-PC, og én var uten restriksjoner. Ved å benytte tildelte testbrukere simulerte testen situasjoner hvor bruker med tilsvarende rettigheter er kompromittert eller forsøkes utnyttes av eksisterende bruker.
[5] Se: https://no.wikipedia.org/wiki/Tjenestenektangrep
[6] Nettfisking benevnes også som «phising» eller «phisking».
[7] Se siste avsnitt av kapittel 5 for mer informasjon om dette.

2. Om tjenesteområdet

2.1 Organisering

Byrådsavdelingen for finans, innovasjon og eiendom (BFIE) ved kommunaldirektør for HR, digitalisering og eiendom har konsernansvaret for informasjonssikkerhet og personvern i Bergen kommune. Seksjon for digitalisering og innovasjon konsern (SDI) i BFIE er overordnet ansvarlig for informasjons- og kommunikasjonsteknologi i Bergen kommune, og har fått delegert sentrale deler av det operative konsernansvaret knyttet til informasjonssikkerhet og personvern.

Figur 1: Organisasjonskart for BFIE[8]



Byrådsavdelingen er organisert med to myndighetsnivåer. Myndighetsnivå 1 omfatter seksjonene og kommunaldirektørene, mens kommunens tjenesteproduksjon og forvaltning hører inn under myndighetsnivå 2, og vil i BFIE blant annet omfatte enhet for digitale tjenester (EDD). EDD er kommunens driftsleverandør innenfor IKT og er tillagt ansvaret for drift av kommunens IKT-systemer og tekniske infrastruktur. EDD har slik en sentral rolle for å sikre den tekniske informasjonssikkerheten i kommunen.

Personvernombudet er del av avdeling for personvern og informasjonssikkerhet som hører inn under SDI. Personvernombudet er en uavhengig instans og rapporterer direkte til kommunaldirektør for HR, digitalisering og eiendom. Inkludert nytt personvernombud er det siden desember 2018 ansatt fire nye stillinger på avdelingen for personvern og informasjonssikkerhet, som nå består av seks ansatte. Fra 1. januar 2019 til 1. april 2019 var en av rådgiverne på avdelingen ansatt som konstituert personvern-ombud.

[8] Kilde: bergen.kommune.no. Kommunen oppgir at organisasjonskartet sist var oppdatert 24. januar 2017.

3. Tilfredsstillende informasjonssikkerhet

3.1 Problemstilling

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

I hvilken grad er det etablert tiltak for å tilfredsstille krav i lovverket knyttet til informasjonssikkerhet?

Under dette:

a) Er det innført rutiner og retningslinjer i samsvar med anbefalingene fra rapporten i 2015, og etterleves disse?
b) I hvilken grad er det gitt føringer for å sikre en helhetlig tilnærming til informasjonssikkerhet i kommunen?

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. 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.

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
    a) risikovurderinger
    b) sikkerhetsrevisjoner
    c) avvikshåndtering
    d) ledelsens gjennomgang

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.

Se vedlegg 2 for utfyllende revisjonskriterier.

3.3 Rutiner og retningslinjer for informasjonssikkerhet

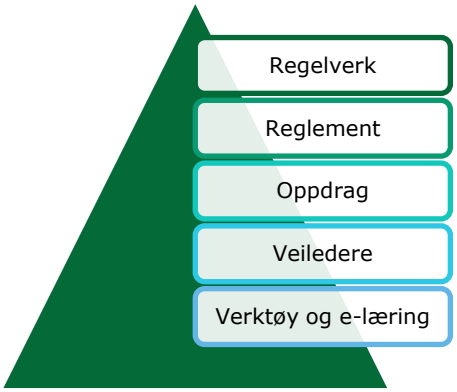
3.3.1 Datagrunnlag

Styrende dokumenter for informasjonssikkerhet

Bergen kommune har gjennom ulike styrende dokumenter etablert et styringssystem for informasjonssikkerhet.[9] 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 figuren under.

Figur 2: Hierarkisk oppbygging av styringssystemet for informasjonssikkerhet og personvern[10]



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. Med andre ord er de behandlingsansvarlige i Bergen kommune kommunaldirektører, bystyredirektør eller direktører for kommunale foretak.

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 kapittel 4).

[9] Benevnelsen på styringssystemet i kommunen er *styringssystem for personvern og informasjonssikkerhet.*
[10] Kilde: Veileder for trygg digitalisering.

Kommunen har også en strategi for informasjonssikkerhet fra 2015. Strategien innledes med et kortfattet sammendrag av viktigheten av informasjonssikkerhet, samt Bergen kommunes visjon for informasjonssikkerhet. Visjonen er at «informasjonssikkerhet og personvern skal være en naturlig del av kommunen».

Strategien har videre et innledningskapittel, som blant annet kort omhandler ulike trusler mot informasjonssikkerhet. I tillegg blir sentrale begreper knyttet til informasjonssikkerhet definert her. Deretter blir regelverket for informasjonssikkerhet kort gjennomgått, med henvisninger til relevant lovverk (personopplysningsloven, kommuneloven, eForvaltningsforskriften) og øvrige føringer, både nasjonale og lokale. Det strategiske fokuset for informasjonssikkerhet blir utdypet i fokusområdene *Organisering og integrasjon* og *Sikkerhetskultur og personvern*, hvert med to delmål.[11]

Avslutningsvis i strategien vises det til at tiltakene BFEE[12] og avdeling for informasjonssikkerhet jobber etter, skal nedfelles i en overordnet handlingsplan for informasjonssikkerhet. I det aktuelle avsnittet vises det til at arbeid med tiltak har utviklet seg siden forrige strategi (2011), og at dette i dag følges opp planmessig og systematisk gjennom balansert målstyring. Videre står det at for å nå målene beskrevet i fokusområdene i strategien, er det avgjørende å gjennomføre de rette tiltakene til rett tid, og å justere tiltakene etter hvert som trusselbildet endrer seg. Revisjonen har ikke opplysninger som tyder på at en slik handlingsplan foreligger, eller at dette blir fulgt opp planmessig og systematisk.

I intervju understrekes det at informasjonssikkerhetsstrategien ble utarbeidet etter forrige byrådsskifte, og at den i dag vurderes som noe utdatert; den er derfor i liten grad styrende for informasjonssikkerhetsarbeidet i kommunen. Direktør for SDI viser til at strategien for digitalisering og innovasjon i Bergen kommune (*Program for digital fornyelse* vedtatt i 2018), har godt personvern og god informasjonssikkerhet som sentrale målsettinger. Denne strategien vurderes som mer relevant og aktuell for informasjonssikkerhetsarbeidet i kommunen.

Videre forteller direktør for SDI at informasjonssikkerhetsstrategien etter planen skal rulleres, ev. utarbeides på nytt, etter kommunevalget i 2019. Kommunen vil i den forbindelse sikre at anbefalingen fra revisjonen i 2015 om at kommunen «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», blir fulgt opp.

I tillegg pekes det på at selv om informasjonssikkerhetsstrategien per i dag i liten grad er styrende for informasjonssikkerhetsarbeidet i kommunen, sammenfaller målsettingene i denne i stor grad med målsettingene i styringssystemet for informasjonssikkerhet og personvern.

Oversikt over personopplysninger

Reglement for trygg digitalisering stiller krav til at den enkelte resultatenhet må ha oversikt over personopplysningene 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.

[11] Delmål 1.1 - Arbeidet med informasjonssikkerhet skal være basert på tydelig organisering, roller, ansvar og tverrfaglig samarbeid; delmål 1.2 - Informasjon skal sikres der det er behov for den, i enhetene; delmål 2.1 - Systematisk samarbeid skal bidra til å minimere risiko for brudd på informasjonssikkerheten; delmål 2.2 - Personvern skal være en synlig del av arbeidet med informasjonssikkerhet.

[12] BFEE er forkortelse for Byrådsavdeling for finans, eiendom og eierskap. Fra 6. oktober 2016 endret denne byrådsavdelingen navn til Byrådsavdeling for finans, eiendom og eiendom (BFIE).

Reglementet viser videre til kommunens intranettside, *Allmenningen,* og siden *Melding om behandling av personopplysninger*.[13] 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 kontaktinformasjon til kommunens personvernombud. Det er også et elektronisk meldeskjema for å melde behandling av personopplysninger på siden.

Revisjonen har fått tilsendt oversikt over innmeldte behandlinger av personopplysninger i Bergen kommune slik dette fremgår i systemet Bk Prosjekt. I oversikten går det frem at det er 347 kjente informasjonssystem i bruk i kommunen, og at det er meldt inn hvilke personopplysninger som blir behandlet i 96 % av disse.[14]

Leder for EDD forteller at det er stilt krav om at alle system som benyttes i kommunen skal meldes inn til dem, men at det fortsatt arbeides med å få full oversikt over alle informasjonssystemene som er i bruk. Han anslår at EDD har oversikt over om lag 95 % av systemene som er i bruk i kommunen. Han forteller at det kan være krevende å holde oversikt over informasjonssystemene ute i enhetene når EDD ikke alltid er involvert i anskaffelsen av systemene, eller når ansatte tar i bruk skybaserte tjenester (for eksempel i skolen). Videre kommer det frem at det kan være informasjonssystemer som fortsatt eksisterer, men ikke lenger er i bruk, og som EDD ikke har oversikt over. I intervju med forhenværende konstituert personvernombud blir det i tillegg pekt på at kommunen nok mangler oversikt over en del mindre informasjonssystemer med avgrenset utbredelse.

Revisjonen har fått tilsendt protokoll med oversikt over personopplysninger som behandles i hver av byrådsavdelingene. Protokollene har samme oppbygging i form av et regneark med en protokollforside og separate regneark med oversikt for hver seksjon/etat/område som inngår i byrådsavdelingen.

Som eksempel har byrådsavdeling for sosial, bolig og inkludering (BSBI) egne oversikter over hvilke personopplysninger som behandles i boligetaten, etat for inkludering, etat for psykisk helse og rus og etat for sosiale tjenester. I oversikten for hvert av områdene går det frem internt ansvarlig, funksjonsområde og hva behandlingen gjelder, i tillegg til 16 andre kategorier som for eksempel formål med behandlingen, behandlingsgrunnlag, system som behandler opplysningene og navn på databehandlere.

Revisjonen blir fortalt at det gjenstår en del arbeid for å få ferdigstilt protokollene med oversikt over alle personopplysninger som blir behandlet av kommunen. Forhenværende konstituert personvernombud anslo at kommunen i disse protokollene hadde oversikt over omlag 95 % av behandlingene som omfatter behandling av personopplysninger om innbyggere i kommunen. Videre blir det opplyst at det ikke er gjennomført revisjoner av noen protokoller ennå, og at dette snart bør gjøres ved de byrådsavdelingene som var tidligst ute med å levere protokoll, for slik å sikre oppdatert og korrekt informasjon i protokollene. I tillegg blir det fortalt at arbeidet med å få oversikt over interne behandlinger av personopplysninger, altså personopplysninger for kommunalt ansatte, på revisjonstidspunktet fremdeles var i oppstartsfasen.

Selv om ansvaret for å føre og ajourholde protokollene ligger til resultatenhetene, er det behov for råd og veiledning fra personvernombudet i gjennomføringen av dette arbeidet (se også kapittel 4).

Melding av avvik som gjelder personvern og informasjonssikkerhet

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 av reglementet at avvik skal meldes i kommunes gjeldende avvikshåndteringssystem og følges opp i samråd med personvernombudet for å avgjøre om avviket skal meldes til Datatilsynet.[15]

---

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

[14] App.powerbi.com (BkProsjekt) [lest 14.08.2019].https://app.powerbi.com/view?r=eyJrIjoiNjVlNTIxZmYtNjM1Zi00NGIzLWEwYzctYzk0NjQyOTgwMjJiIiwidCI6ImQ0MWNhYWE5LWE0MWEtNGUwZi05YmY2LTA1Y2QxZjQ4ZDI3MSIsImMiOjh9&pageName=ReportSection07603637e1745cb2545a

[15] Som del av styringssystemet for personvern og informasjonssikkerhet har kommunen utarbeidet en mal for personvernombudets vurdering av personvernkonsekvenser for avvik, som forklarer hvorfor og hvordan personvernombudet skal vurdere avvik (datert 12.10.2018).

Revisjonen har videre fått tilsendt en *Overordnet rutine for håndtering av avvik som gjelder personvern og informasjonssikkerhet*.[16] Denne er felles for alle i kommunen. I denne fremgår blant annet ansvarsfordeling og saksgang knyttet til avviksmeldinger som gjengitt i tabell 3:

Tabell 3: 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

Bergen kommune har innført nytt kvalitetssystem (Bk Kvalitet) fra 1. januar 2019.[17] Kvalitetssystemet har en egen avviksmodul. Denne avviksmodulen er felles for hele kommunen, og skal benyttes ved melding av alle typer avvik, inkludert informasjonssikkerhetsavvik.[18]

Rutinen for håndtering av avvik viser ikke til det nye kvalitetssystemet, men beskriver at ansatte skal melde avvik skriftlig eller muntlig til enhetsleder og at enhetsleder etter vurdering av videre håndtering skal fylle ut elektronisk skjema som skal sendes til avdeling for personvern og informasjonssikkerhet.[19]

På *Allmenningen* er det lagt inn informasjon om avvikshåndtering knyttet til personvern og informasjonssikkerhet. 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 avvik via kvalitetssystemet og lenke til den overordnede rutinen for avvik.

I spørreundersøkelsen som er gjennomført i forbindelse med forvaltningsrevisjonen, svarer 33 % at de *ikke* kjenner til rutinene for å melde avvik knyttet til informasjonssikkerhet.[20] På samme spørsmål i 2014 svarte 62 % av respondentene at de ikke kjente til disse rutinene (se også seksjon 5.3).[21]

I intervju blir det vist til at det nye kvalitetssystemet gjør det enklere å finne frem til hvor og hvordan man skal melde avvik, og at det er mindre feilrapportering enn før. Dette blir underbygget med at det i første kvartal i 2019 ble meldt flere informasjonssikkerhetsavvik enn i hele 2018.

Forhenværende konstituert personvernombud opplever, basert på innmeldte avvik, at ansatte i kommunen har er bevisst forhold til informasjonssikkerhet, også utover det som knytter seg til personvern og

[16] Overordnet rutine for håndtering av avvik som gjelder personvern og informasjonssikkerhet. Revisjonsdato 31.01.2018. Gyldig til 28.02.2019.
[17] Kvalitetssystemet er basert på Extend Quality System (EQS).
[18] Det blir nevnt at Bergen Vann, vann- og avløpsetaten og etat for bygg og eiendom benytter et eget avvikssystem. Lederne av disse enhetene har blitt fortalt at avvik knyttet til informasjonssikkerhet skal meldes i Bk Kvalitet.
[19] Den overordnede rutinen viser heller ikke eksplisitt til kommunens intranettsider, men informasjonen om at enhetsleder skal melde avvik via elektronisk skjema er lenket til intranettsiden som omhandler avvikshåndtering.
[20] N=380.
[21] Spørreundersøkelsen som ble gjennomført i 2019 hadde svaralternativet «delvis», noe som ikke var inkludert i undersøkelsen i 2014. Dette påvirker sannsynligvis prosentfordelingen på ja/nei.

personopplysninger.[22] Han vedgår likevel at det mest sannsynlig er store mørketall i kommunen når det gjelder faktiske avvik knyttet til informasjonssikkerhet sett opp mot innmeldte avvik.

Revisjonen har fått tilsendt oversikt over avvik knyttet til informasjonssikkerhet og personvern meldt mellom 20. juli 2018 til 5. mars 2019. Det fremgår av oversikten at det i tidsperioden ble meldt 58 avvik av denne typen,[23] hvorav 39 ble meldt fra byrådsavdeling for helse og omsorg (BHO).[24]

Til sammenligning ble det mellom 6. mars og 7. august 2019 meldt 81 avvik knyttet til informasjons-sikkerhet, fordelt på underkategorier som vist i tabell 4:

Tabell 4: Avviksstatistikk informasjonssikkerhet (mars-august 2019)[25]

Underkategori	Antall
Observasjoner[26]	29
Midlertidig eller permanent tap av informasjon	20
Ulovlig behandling av personopplysninger	13
Uønsket endring i informasjon	2
Uønsket innsyn i informasjon	17
Sum	**81**

Risikovurderinger

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 intranettsidene. På intranettsidene fremgår det 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.

Revisjonen har fått tilsendt skjema for overordnet risiko- og sårbarhetsanalyse (ROS) for uke 11 i 2019 knyttet til informasjonssikkerhet og personvern i kommunen. I oversikten blir akseptkriteriene kritisk-, høy-, moderat- og lav risiko beskrevet (gjengitt i tabell 5):

[22] Han nevner som eksempel at det blir meldt avvik på at utskrifter blir liggende for lenge i skriverne.
[23] Oversikten viste 65 avvik, men 7 av disse omhandlet HMS eller kvalitet og ikke informasjonssikkerhet.
[24] I fire av avvikene som ble meldt var ikke byrådsavdeling registrert.
[25] Kilde: Bk Kvalitet.
[26] Observasjonene er avvik knyttet til farlige forhold eller forhold som har forbedringspotensial, men ikke faktiske uønskede hendelser.

Tabell 5: Akseptkriterier for overordnet ROS

Risikonivå	Beskrivelse	Akseptabelt?
Kritisk risiko	Kritisk risiko betyr at det er stor sannsynlighet for at hendelsen inntreffer, og at det i så fall vil få store konsekvenser.	Nei, strakstiltak for å redusere risiko må iverksettes snarest, følges opp, overvåkes og vurderes fortløpende.
Høy risiko	Høy risiko betyr at det er liten sannsynlighet for at hendelsen inntreffer, men at det kan få store konsekvenser hvis det skjer likevel.	Midlertidig, tiltak for å redusere risiko må planlegges, følges opp, overvåkes og vurderes fortløpende.
Moderat risiko	Moderat risiko betyr at det er stor sannsynlighet for at hendelsen inntreffer, men at konsekvensene er små.	Ja, men risikoreduserende tiltak bør følges opp og vurderes jevnlig.
Lav risiko	Lav risiko betyr at det er liten sannsynlighet for at hendelsen inntreffer og at konsekvensene i så fall er små.	Ja, men iverksatte tiltak overvåkes likevel jevnlig.

I skjemaet er det et ark der overordnet etterlevelse knyttet til uønskete hendelser blir beskrevet og vurdert opp mot akseptkriteriene. I tilsendt skjema er det eksempelvis lagt inn en uønsket hendelse; «manglende eller mangelfull vurdering av risiko for brudd på personopplysningssikkerheten», etterfulgt av beskrivelse av risikoen og en vurdering av risiko som «kritisk». Det er lagt inn tiltaksreferanse på hver av de uønskede hendelsene.

Videre inneholder skjemaet et ark hvor det er registrert uønskede hendelser, beskrivelse av risiko, vurdering av risiko og tiltaksreferanse fordelt på ansvarlig leder eller enhet, i dette tilfellet resultatenhets-leder, systemeier og EDD. I siste del av skjema er det lagt inn en tiltaksoversikt hvor det er lagt inn tiltak, hvem som er ansvarlig for tiltaket, frist for ferdigstilling, status for gjennomføring og ev. kommentarer.

I intervju blir det fortalt at arbeidet med felles system for risikovurderinger har kommet i gang, men at det ikke ennå er helt på plass. Revisjonen får videre opplyst at det er gjennomført et stort antall risikovurderinger siste periode, med utgangspunkt i innmeldte behandlinger av personopplysninger. Fra tilsendt oversikt over kartlegging av behandlinger av personopplysninger i systemet BK Prosjekt, går det frem at 160 av de 347 kjente systemene der det behandles personopplysninger er ferdig risikovurdert. Dette utgjør om lag 46 %. Videre kommer det frem i intervju at ikke alle risikovurderingene er fullstendige; for en del av dem mangler for eksempel tekniske vurderinger og infrastrukturvurderinger.

Videre blir det fortalt at EDD har pågående en risikovurderingsprosess der de har risikovurdert elevnettet, sikker sone, det administrative nettet, samt infrastrukturen i kommunen. Det fremgår videre at EDD, i samarbeid med byrådsavdelingene, har gjort kritikalitetsvurderinger av flere systemer, og at det foreligger en prioritert liste over systemer som må prioriteres ved hendelser og nedetid.

Vurdering av personvernkonsekvenser (DPIA)

I *Veileder for trygg digitalisering* fremgår det at det skal foretas en vurdering av personvernkonsekvenser (DPIA)[27] når det utvikles nye system, både ved oppstart av utviklingen og underveis i utviklingsprosessen.

Videre står det at den behandlingsansvarlige skal rådføre seg med personvernombudet ved vurdering av personvernkonsekvens.

I veilederen vises det videre til at personvernombudet, sammen med flere kommuner, er i gang med å utvikle et verktøy for å vurdere personvernkonsekvens. Veilederen har ikke lenker eller forklaring til hvor man kan finne utfyllende informasjon om hvordan å gjennomføre slik vurdering.

I kommunen sin *Veileder for ledere knyttet til personvern og informasjonssikkerhet* fremgår i hovedsak de samme opplysningene om DPIA som beskrevet i *Veileder for trygg digitalisering* (som vist i avsnittet over). I tillegg er det lagt inn en lenke til et «spørreskjema» (vurdering av personvernkonsekvenser (DPIA)) som bør benyttes for å avgjøre om det er nødvendig med vurdering av personvernkonsekvenser.

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

Kommunens intranett har en temaside som omhandler personvernkonsekvensvurdering som inneholder informasjon om hva en DPIA er, hva den skal inneholde, når man skal gjennomføre DPIA, liste over behandlingsaktiviteter som alltid krever DPIA, samt om personvernombudets rolle i forbindelse med utførelsen av DPIA. Det er videre lagt inn lenke til skjema for initiell vurdering av behovet for utførelse av DPIA på denne intranettsiden («Del 1»). I selve skjemaet skal man blant annet svare ja/nei på spørsmål knyttet til *proporsjonalitet* knyttet til behandling av personopplysninger, for eksempel om det er absolutt nødvendig å behandle personopplysninger for å nå formålet. Videre skal man svare ja/nei på 9 spørsmål om hva behandlingen av personopplysninger innebærer for deretter å kunne identifisere om det er behov for DPIA. Det fremgår av skjema at dersom det er to eller flere «ja» på spørsmål 1-9, eller dersom behandlingen involverer innovativ bruk av ny teknologi, skal DPIA gjennomføres.

Revisjonen har fått tilsendt et *DPIA-verktøy* som inneholder det ovennevnte skjema for vurdering av DPIA, samt verktøy for del 1 og 2 av konsekvensutredning og mal for rapport. I del 1 av konsekvensutredningen skal man ved hjelp av et flytskjema beskrive behandlingen av personopplysninger i praksis, beskrive hvordan behandlingen er avgrenset til det som er absolutt nødvendig, samt fylle ut et skjema knyttet til om/hvordan behandlingen ivaretar rettigheter for den registrerte (fortrolighet, riktighet, tilgjengelighet, åpenhet, påvirkning, koblingsfrihet). Del 2 av konsekvensutredningen er tilsvarende del 1, og skal fylles ut dersom det er endringer i behandlingen av personopplysninger.

Det er ikke lenke til DPIA-verktøyet på kommunen sine intranettsider som omhandler tema.

Revisjonen har også fått tilsendt en oversikt over gjennomførte og pågående DPIA i kommunen. I denne oversikten fremgår det at det er gjennomført DPIA for elektronisk elevmapper, risikobasert tilsyn i bolig,[28] register for parkeringstillatelser for forflytningshemmede (HC-register), fagsystemet Profil og Geriatrisk Basis Datasett (GBD), og at det er en pågående DPIA for HMSReg.[29]

Personvernerklæring

Bergen kommune har en personvernerklæring som ligger tilgjengelig nederst på kommunens hjemmeside.[30] På samme siden finner man også informasjon om personvernombud og informasjonskapsler.

Innledningsvis i erklæringen går det frem at kommunen har mål om at informasjonssikkerhet og personvern skal være en naturlig del av virksomheten i kommunen, før det blir gitt en kort introduksjon til erklæringen. Erklæringen er delt inn i 15 seksjoner, med overskrifter som for eksempel «Grunnprinsipper», «Formål», «Innsyn», «Dataportabilitet» og «Protokoll over behandling av personopplysninger». Under hver overskrift følger det kortfattede forklaringer, og i flere er det lagt inn lenke til personopplysningsloven og aktuelle artikler i personvernforordningen.

Under overskriften *Protokoll over behandling av personopplysninger* er det også lagt inn lenke til protokoll fra Byrådsavdelingen for helse og omsorg, Byrådsavdelingen for klima, kultur og næring og Byrådsavdelingen for barnehage, skole og idrett. Det er ikke publisert protokoller fra de andre byrådsavdelingene, men det går frem av siden at dette skal blir gjort «fortløpende».[31] I forbindelse med verifiseringen av rapporten blir det pekt på at det ikke er noe krav om å publisere slike protokoller, men at Bergen kommune har tatt et valg om å være åpen og transparent om sine behandlinger av personopplysninger.

Kontroll og revisjon

Kommunens *Reglement for trygg digitalisering* slår fast at «arbeidet med personvern og informasjonssikkerhet skal være gjenstand for oppfølgning, regelmessig kontroll og revisjon for å sikre etterlevelse, både internt i den enkelte virksomhet og fra overordnet nivå». To punkt blir spesielt fremhevet:

[28] Tilsyn ihht forskrift om brannforebygging i bolig
[29] Planlagt oppstart 11. eller 12. april 2019. HMSReg er et informasjonssystem som gir oversikt over anleggslokasjoner og hvilke leverandører og mannskap som er til stede. Revisjonen har fått tilsendt gjennomført DPIA for de tre førstnevnte systemene, men ikke for fagsystemet Profil og GBD. Kommunen opplyser at gjennomføringen av DPIA for Profil og GBD ble utført utelukkende for å ha en «systematisk tilnærming til problemstillinger».
[30] «Personvern og informasjonskapsler»: https://www.bergen.kommune.no/omkommunen/personvern/11992
[31] https://www.bergen.kommune.no/omkommunen/personvern [lest 01.08.2019].

- Enhver kommunaldirektør skal delta med en representant i informasjonssikkerhetsforum, kommunens organ for oppfølging av arbeidet med personvern og informasjonssikkerhet.
- Kommunaldirektør skal minimum årlig gjennomføre ledelsens gjennomgang og gjøre opp status på arbeidet med personvern og informasjonssikkerhet i samråd med kommunens personvernombud.

Det står videre at informasjonssikkerhetsforum skal møtes minimum kvartalsvis og at personvernombudet årlig, eller oftere ved særskilte behov, skal rapportere til kommunens øverste ledelse.

I *Veileder for trygg digitalisering*[32] står det at kommunen skal identifisere nødvendige tiltak for deretter å planlegge, gjennomføre og kontrollere tiltakene for å avdekke om de oppfyller formålet. Videre står det beskrevet at resultatet fra tiltakene har som hovedformål å gi styringssignaler tilbake til styringssystemet for å revidere og justere strategiske mål og underliggende dokumenter. Veilederen går videre inn på de ulike områdene for kontroll og revisjon som skal utføres i kommunen; egenkontroll, sikkerhetsrevisjon og ledelsens gjennomgang:

Ledelsens gjennomgang
Kommunens *Veileder for trygg digitalisering* omtaler «ledelsens gjennomgang». Det fremgår blant annet at sikkerhetsforum årlig skal rapportere resultatet av sitt arbeid til kommunens øverste ledelse.

I *Mandat for informasjonssikkerhetsforum*[33] blir det gjort rede for bakgrunnen for opprettelse av informasjonssikkerhetsforum, samt formålet, sammensetning, faste oppgaver og møtefrekvens for forumet. Forumet ledes av kommunaldirektør for HR, digitalisering og eiendom. De øvrige kommunaldirektørene i kommunen skal stille med én representant hver. Andre faste medlemmer er personvernombudet med rådgivere og representanter fra SDI, HR konsern, EDD (operativ sikkerhetsansvarlig) og samfunnssikkerhet og beredskap.

Kommunen har videre utarbeidet en *Prosedyre for ledelsens gjennomgang*[34] der formål og hjemmel fremgår innledningsvis. Deretter blir det slått fast hva som er bakgrunnen for ledelsens gjennomgang:

> å belyse status på arbeidet med informasjonssikkerhet og personvern i byrådsavdelingene og å gi kommunaldirektørene tilstrekkelig styringsinformasjon til å ta nødvendige avgjørelser.

Videre viser prosedyren til hvilke punkter personvernombudet skal gå gjennom ved ledelsens gjennomgang og deretter at målet for gjennomgangen er at kommunaldirektør beslutter plan for videre arbeid på området i egen byrådsavdeling.

Revisjonen har fått tilsendt de gjennomførte gjennomgangene for ledelsen for 2018[35] i samtlige byrådsavdelinger i kommunen. De tilsendte gjennomgangene har felles oppsett der personvernombudet rapporterer om funn og status knyttet til informasjonssikkerhet på byrådsavdelingene, med følgende hovedpunkt:

- Gjennomgang av relevante lov- og regelverkshendelser
- Gjennomgang av offentlig protokoll for behandling av personopplysninger
- Resultat fra revisjoner og kontroller i byrådsavdelingen[36]
- Gjennomgang av trusselbildet for personvern og informasjonssikkerhet
- Gjennomgang av vesentlige avviksaker i byrådsavdelingen
- Forslag til plan for videre arbeid med personvern og informasjonssikkerhet
- Mål

Revisjonen får opplyst i intervju at det ikke har vært arbeidet systematisk med ledelsens gjennomgang i kommunen de siste årene. Det blir vist til at informasjonssikkerhetsforum, etter at det ble reetablert høsten

[32] Veileder for trygg digitalisering. Styringssystem for personvern og informasjonssikkerhet. Bergen kommune.
[33] Mandat for informasjonssikkerhetsforum. Revisjonsdato 05.09.2018. Gyldig til 13.09.2019.
[34] Prosedyre for ledelsens gjennomgang. Revisjonsdato 04.09.2018. Gyldig til 13.09.2019.
[35] I intervju blir det fortalt at ledelsens gjennomgang for 2018 ble sluttført noe forsinket gjennom informasjonssikkerhetsforum i mai 2019.
[36] Knyttet til resultater fra revisjoner og kontroller, samt status på arbeid med oppfølging er dette satt som «ikke aktuelt» i BORG, BLED, BBU, BKKN, BSBI, BHO, mens det for BBSI og BFIE er lagt inn kommentar om at de vil omfattes av forvaltningsrevisjoner i løpet av 2019.

2018, er et viktig møtested knyttet til ledelsens gjennomgang, og at det gjennom dette forumet blir rapportert videre til ledelsen i hver byrådsavdeling om arbeid knyttet til informasjonssikkerhet.

Sikkerhetsrevisjon og egenkontroll
Kommunens *Veileder for trygg digitalisering* slår fast at personvernombudet med ujevne mellomrom og i henhold til rettslige krav, skal gjennomføre ulike former for sikkerhetsrevisjoner i samarbeid med seksjon for internkontroll. Videre blir formålet med sikkerhetsrevisjoner kort gjort rede for:

> å avdekke forbedringspunkter og avvik, og bidra til kontinuerlig forbedring og kvalitetssikring av arbeidet med personvern og informasjonssikkerhet.

Det står videre i veilederen at alle resultatenhetsledere skal rapportere status gjennom kommunens årlige sjekkliste for internkontroll,[37] og videre at sikkerhetsforum skal følge opp egenkontrollen med stikkprøve-baserte internrevisjoner som skal dokumenteres i en revisjonsrapport.

Revisjonen har fått tilsendt utkast til rapport etter seksjon for internkontrolls gjennomgang av SDIs forvaltning av konsernansvaret for informasjonssikkerhet i 2018,[38] samt SDIs tilbakemeldinger på utkastet og en handlingsplan for seksjonen basert på funn i internkontrollrapporten. I handlingsplanen er det satt opp 28 punkt med iverksatte tiltak, noen med tidsfrist for gjennomføring og med merknad til 26 av 28 punkter.

Revisjonen har videre fått tilsendt oversikt over revisjoner og testing av informasjonssikkerhet som har blitt gjennomført i kommunen de siste årene. I denne går det frem at kommunen både har gjennomført sikkerhetsrevisjoner, inntrengningstester og IT-revisjoner, noen i egenregi og andre utført av eksterne. Det er ikke gjennomført sikkerhetsrevisjon som egenkontroll siden 2016. I intervju blir det opplyst at avdeling for personvern og informasjonssikkerhet har planlagt å gjennomføre en sikkerhetsrevisjon i løpet av 2019. Videre understrekes det i intervju at temaene personvern og informasjonssikkerhet er inkludert i kommunens årlige internkontrollundersøkelse og at avdeling for personvern og informasjonssikkerhet har etablert et samarbeid med seksjon for internkontroll.

Tilgangsstyring

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

Som nevnt tidligere i rapporten blir det i *Reglementet for trygg digitalisering* definert 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 og informasjonssikkerhet følges opp i egen resultatenhet. Det vises deretter til oppdrags-beskrivelse for resultatenhetsledere knyttet til informasjonssikkerhet.[39] I denne oppdragsbeskrivelsen fremgår det at resultatenhetslederne har ansvar for tilgang i informasjonssystemene knyttet til risiko-vurdering, avviksmelding og beredskap:

- 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 uvedkommende.

Det fremgår ikke hva som er rutiner, eller lenke til rutinebeskrivelser, for arbeidet med tilgangsstyring i oppdragsbeskrivelsen for resultatenhetsledere. Dette er imidlertid tilgjengeliggjort på kommunens intranett; på *Allmenningen* er det under *Ansatthjelpen*, *Informasjonstjenester og IKT* og *Systemer,*

[37] På *Allmenningen* står det at seksjon for internkontroll årlig utarbeider en generell sjekkliste for internkontroll som dekker fellesprosessene risikostyring, HR/HMS, lønn og refusjon, regnskap og budsjett, innkjøp og informasjonssikkerhet.
[38] Utkast rapport: Forvaltning av konsernansvar for informasjonssikkerhet. Byrådsleders avdeling – Seksjon for internkontroll. 25. juni 2018.
[39] Oppdrag – personvern og informasjonssikkerhet for resultatenhetsledere. Ikke datert

tilganger og passord flere sider som omhandler tilganger til kommunens informasjonssystemer. Sentralt blant disse er siden *Bestille, endre og slette brukerid/brukertilgang*. 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 blir i intervju opplyst at det er nærmeste leder som bestiller tilganger til ansatte gjennom Bestillingsweb. Videre blir det opplyst at når en ansatt er opprettet i lønnssystemet, får EDD melding og oppretter sentral brukerkonto.[40] I intervju fremholdes det at risikoen for at ansatte får tildelt tilganger de ikke skal ha ved ansettelse er liten. Det kan imidlertid skje at ikke alle tilgangene er på plass fra dag én.

Det fremgår i intervju at prosessen for tilgangsbestilling til nyansatte kan bedres for å sikre kvaliteten for nyansatte og å lette prosessen for ledere.

Revisjonen har òg fått tilsendt kommunens *Sjekkliste for leder ved avslutning av arbeidsforhold*.[41] Under overskriften *IKT* fremgår det hvilke aktiviteter leder skal gjennomføre, beskrivelse av hvordan det skal utføres og i noen tilfeller lenker til skjema og system som skal benyttes. Blant aktivitetene som beskrives er avbestilling/deaktivering av tilgang til fagsystem, overføring av tjenstlig informasjon/pågående saker til fellesområder og oppheving av systemtilganger. Under overskriften *annet* blir det videre beskrevet at leder må sørge for at ID-kort, nøkler og lignende tilbakeleveres.

På den ovenfor nevnte siden på *Allmenningen* er det beskrevet rutiner for hva ansvarlig leder skal foreta seg med hensyn til tilganger til informasjonssystemer; dette skal ansvarlig leder melde fra om via Bestillingsweb, for at brukerkonto deaktiveres og eventuelle tilganger til fagsystemer og filområder fjernes.[42]

I intervju gis det uttrykk for at prosessen knyttet til tilganger når en ansatt slutter fungerer bra. Det blir fortalt at de fleste systemene i kommunen går gjennom *single sign-on*, noe som betyr at når en brukerkonto er deaktivert i det sentrale systemet, får ikke vedkommende logget på datamaskinen sin, og mister dermed også tilgang til informasjonssystemene.[43]

Det fremgår i intervju at det er risiko for at tilganger ikke avsluttes dersom ansatte endrer stilling innad i kommunen. Det blir fortalt at brukerkontoer automatisk blir flyttet i det sentrale systemet når en ansatt endrer stilling,[44] men at ikke alle tilganger følger automatisk i denne prosessen. Det understrekes i intervju at det er systemeiere som skal følge opp at ansatte ikke har unødvendige tilganger til systemet.

Også skifte av arbeidssted i kommunen er omtalt på intranettsiden *Bestille, endre og slette brukerid /brukertilgang*. Ansatte skal da melde fra til nåværende leder, og har selv ansvar for å sikre at relevant informasjon overføres. Nåværende leder skal gjennom Bestillingsweb fjerne tilganger som den ansatte ikke lenger skal ha, mens ny leder samme sted skal bestille nye tilganger.

Leder for EDD opplever at EDD håndterer sitt ansvar for konfidensialitet og integritet på en god måte, men forteller at det er vanskelig å si noe sikkert om hvordan dette blir etterlevd ute i enhetene. Han nevner videre at et av tiltakene som for tiden blir gjennomført i kommunen for å sikre konfidensialitet er to-faktorautentisering for å logge seg inn på kommunen sine informasjonssystemer.

Sikkerhet

For å undersøke kommunens tekniske informasjonssikkerhet, har revisjonen gjennomført sikkerhetstester i ulike deler av kommunens IKT-system. Sikkerhetstestene ble gjort både fra utsiden (internett) og innsiden (intranett) av kommunens nettverk.

---

[40] I Active Directory (AD).
[41] Avslutning av arbeidsforhold. Sjekkliste for leder. Revidert 08.06.2017.
[42] Denne aktuelle rutinene gjelder også for ansatte som skal i permisjon.
[43] E-postbokser blir slettet tre måneder etter at brukerkontoen er deaktivert. Dersom en bruker er inaktiv i tre måneder går det ut melding til bruker, og dersom en brukerkonto er inaktiv i et halvt år blir den avsluttet.
[44] Til en ny såkalt *organizational unit* (OU) i AD-terminologi.

For den eksterne testen fikk revisjonen tilsendt oversikt over hvilke internettadresser kommunen eier, og gjorde så undersøkelser for å kartlegge hvilke ressurser som er tilgjengeliggjort mot internett på disse. Deretter ble åpne porter, tilgjengelige tjenester og benyttete protokoller identifisert, og det ble gjennomført analyser av eventuelle feilkonfigurasjoner og manglende sikkerhetsoppdateringer blant de identifiserte tjenestene.

Den interne 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.

Det primære fokuset til den interne sikkerhetstesten var å avdekke hvorvidt eksisterende sikkerhets-kontroller og/eller filtreringsmekanismer (primært brannmur) 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 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.

Både de eksterne og interne sikkerhetstestene ble gjennomført delvis manuelt, og delvis ved bruk av ulik spesialisert programvare. For nærmere tekniske beskrivelser av testene vises det til vedlegg 5.

Funn og sårbarheter identifisert i testene ble kategorisert etter risiko (tabell 6).

Tabell 6: Risikovurdering

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

Risikoen er beregnet ut i fra estimert *konsekvens* (tabell 7) og *sannsynlighet* (tabell 8).

Tabell 7: Rangering av sårbarheter etter konsekvens

- **Høy:** 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:** 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:** 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.

Tabell 8: Rangering av sårbarheter etter sannsynlighet

- **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.
- **Moderat:** Utnyttelse av disse sårbarhetene er mer sofistikert. Disse 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.
- **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.

Den eksterne testen avdekket ingen sårbarheter med kritisk eller høy risiko, men det ble identifisert tre sårbarheter med lav risiko, og syv med medium risiko.

Den interne sikkerhetstesten avdekket ingen 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.

Se vedlegg 5 for detaljer.

3.3.2 Vurdering

Gjennom *Reglement for trygg digitalisering* med tilhørende prosedyrer, rutiner og retningslinjer, har Bergen kommune styrende dokumenter for informasjonssikkerhet. Dokumentene refererer til det nye regelverket fra juli 2018, og viser videre til andre relevante regelverk og anbefalinger. Revisjonen er oppmerksom på at *Reglement for trygg digitalisering* og de andre dokumentene som sammen utgjør kommunens styringssystem for personvern og informasjonssikkerhet ble vedtatt og implementert relativt nylig. Basert på funnene i undersøkelsen har likevel revisjonen ingen indikasjoner på at Bergen kommune sine styrende dokumenter ikke er i samsvar med kravene i gjeldende regelverk.

Oppfølging av anbefalingene fra 2015

Kommunen har gjennom utarbeidelsen og implementeringen av nytt styringssystemet for personvern og informasjonssikkerhet utbedret flere av svakhetene påpekt i revisjonen fra 2015.

Kommunen har etablert prosedyre for behandling av **avvik** som blant annet sier at personopplysningsavvik skal meldes til Datatilsynet innen 72 timer, slik det er stilt krav om personvernforordningen artikkel 33 nr. 1. Videre blir det meldt informasjonssikkerhetsavvik i kommunens avvikssystem. Svarene i spørreundersøkelsen tyder imidlertid på at en relativt stor andel ansatte i kommunen ikke vet at de skal melde informasjonssikkerhetsavvik når de opplever eller observerer slike. Dette gir risiko for at avvik ikke blir meldt. Revisjonen er oppmerksom på at kommunen relativt nylig innførte det nåværende avvikssystemet, og registrerer videre at antallet avvik har økt etter det. Likevel mener revisjonen at både svarene i spørreundersøkelsen og antallet meldte informasjonssikkerhetsavvik tyder på at avvik ikke blir meldt. Revisjonen vil i den sammenheng peke på at manglende avviksmeldinger øker risikoen for at svakheter i systemene

ikke blir rettet. Revisjonen mener at kommunen sin avvikspraksis ikke fullt ut er i samsvar med anbefalingene i ISO27001:2013 eller generelle prinsipp for god internkontroll.

Undersøkelsen viser at kommunen har etablert verktøy og retningslinjer for gjennomføring av **risikovurderinger** knyttet til informasjonssikkerhet, og videre at det blir gjennomført risikovurderinger knyttet til informasjonssikkerhet. Det gjenstår imidlertid en del på den faktiske gjennomføringen av risikovurderinger for at kommunen skal få fullstendig oversikt over hvor det er informasjonssikkerhetsrisikoer. Selv om kommunen siden 2015 har gjort fremskritt med hensyn til dette, viser undersøkelsen at over halvparten av systemene fortsatt ikke er risikovurdert, og videre at en del gjennomførte risikovurderinger ikke er fullstendige.

Manglende og mangelfulle risikovurderinger gjør at kommunen ikke har tilstrekkelig oversikt over hvor det er informasjonssikkerhetsrisikoer, og kommunen vet derfor heller ikke hvilke eventuelle sikkerhetstiltak som fungerer og hvilke som ikke fungerer. Kommunen mangler med dette grunnlag for å gjøre eventuelle justeringer og slik kontinuerlig forbedre informasjonssikkerheten.

Bergen kommune har i sine styrende dokumenter for informasjonssikkerhet formalisert krav om gjennomføring av **sikkerhetsrevisjoner**. Undersøkelsen viser videre at det siden 2015 har blitt gjennomført en rekke revisjoner og tester av informasjonssikkerheten til kommunen, både i egenregi og utført av eksterne. I tillegg kommer det frem at seksjon for internkontroll har gjort en gjennomgang av konsernansvaret for informasjonssikkerhet i kommunen, samt at avdeling for personvern og informasjonssikkerhet har planlagt å gjennomføre en sikkerhetsrevisjon i løpet av 2019.

Revisjonen stiller imidlertid spørsmål ved om omfanget av sikkerhetsrevisjoner er tilstrekkelig for å avdekke eventuelle vesentlige sikkerhetsbrister, og slik kunne iverksettes tiltak for å utbedre disse. Som nevnt over, har ikke kommunen gjennomført tilstrekkelig risikoanalyser til å ha fullstendig oversikt over hvor det er risiko for brudd på informasjonssikkerhet. Kommunen mangler derfor også grunnlag for å velge ut de områdene og systemene for sikkerhetsrevisjon der risikoen for brudd på informasjonssikkerheten er størst.

Undersøkelsen viser at kommunen stiller krav til og har utarbeidet prosedyrer for gjennomføring av **ledelsens gjennomgang**. Videre viser undersøkelsen at det per byrådsavdeling ble gjennomført ledelsens gjennomgang for 2018. Gjennom reetableringen av informasjonssikkerhetsforum høsten 2018 har kommunen i tillegg fått på plass de organisatoriske forutsetningene for å kunne gjennomføre ledelsens gjennomgang på overordnet nivå, og revisjonen har informasjon om at dette ble gjort i 2019.

Revisjonen registrerer at anbefaling 4 fra 2015, om at det 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» i liten grad er fulgt opp; kommunen har etablert en informasjonssikkerhetsstrategi, men denne er ikke styrende for informasjonssikkerhetsarbeidet i kommunen. I tillegg blir oppfølging av og rapportering på gjennomføring av tiltak ikke eller i liten grad gjort. Revisjonen merker seg at kommunen har plan om å rullere eller ev. utarbeide ny informasjonssikkerhetsstrategi, og derigjennom følge opp anbefalingen fra 2015.

Tilgangsstyring og sikkerhet

Undersøkelsen viser at Bergen kommune har system og rutiner for tilgangsstyring. Basert på det som kommer frem i revisjonens undersøkelse – blant annet at det i intervju pekes på at prosessen knyttet til dette har forbedringspotensial – vurderes disse bare i noen grad å være egnet til sikre at ansatte i kommunen får tilgangene de trenger, og for å sikre at ansatte som slutter i kommunen mister tilgangene sine. Kommunens rutine og praksis knyttet til tilgangsstyring ved internt skifte av arbeidssted i kommunen vurderes videre som sårbar; her pålegges både den ansatte, forhenværende og ny leder oppgaver, og undersøkelsen viser videre at de tekniske løsningene ikke sikrer at alle tilganger avsluttes eller flyttes automatisk selv om rutinene følges.

Undersøkelsen viser videre at mye av ansvaret knyttet til tilgangsstyring ligger hos ledere og systemeiere. Sett i sammenheng med funn i kapittel 4 knyttet til resultatenhetsledere og systemeieres delvis manglende oppfyllelse av eget informasjonssikkerhetsansvar, mener revisjonen det er risiko for at ansatte i kommunen har tilganger de ikke skulle hatt, og videre at kommunen bør iverksette tiltak for å redusere denne risikoen.

De gjennomførte sikkerhetstestene avdekket ingen kritiske sårbarheter i kommunens eksterne eller interne nett. Det ble imidlertid identifisert sårbarheter med både høy, moderat og lav risiko. Disse medfører risiko for brudd på informasjonssikkerheten i kommunens informasjonssystemer, både knyttet til konfidensialitet, tilgjengelighet og integritet. Revisjonen mener kommunen må iverksette tiltak for å redusere disse. For tekniske detaljer knyttet til dette, viser revisjonen til funn og vurderinger i vedlegg 5.

Etterlevelse av nye lovkrav

Bergen kommune har etablert system og praksis for melding om behandling av personopplysninger og utarbeidelse av **protokoller** med oversikt over slike behandlinger. I undersøkelsen kommer det frem at byrådsavdelingene har utarbeidet protokoller med oversikt over behandlinger av personopplysninger. Revisjonen merker seg imidlertid at disse er i ulik grad av ferdigstillelse, og videre at kommunen ikke har fullstendig oversikt over alle systemene der det muligens behandles personopplysninger. Uten fullstendig oversikt over hvilke systemer der det behandles personopplysninger, kan ikke kommunen ha fullstendige protokoller over behandlinger. I tillegg kommer det frem i undersøkelsen at kommunen ikke har fullstendig oversikt over interne behandlinger av personopplysninger. Manglende fullstendighet i oversikt og protokoller gjør at kommunen ikke fullt ut oppfyller kravet i personvernforordningen artikkel 30 nr. 1, om å føre protokoll over utførte behandlingsaktiviteter av personopplysninger.

Revisjonen har ikke informasjon som tyder på at kommunens retningslinjer, rutiner og verktøy for **vurdering av personvernkonsekvenser** bryter med kravene i regelverket. Undersøkelsen viser videre at kommunen har gjennomført noen vurderinger av personvernkonsekvenser. Revisjonen vil likevel peke på at manglende risikovurderinger kombinert med mangelfull oversikt over hvilke personopplysninger som behandles (se over) gjør at kommunen ikke har full oversikt over hvilke personopplysninger som behandles med høy risiko. Kommunen har derfor heller ikke et tilstrekkelig kunnskapsgrunnlag for å gjennomføre vurdering av personvernkonsekvenser ved behandling av personopplysninger med høy risiko, jf. personvernforordningen artikkel 35.

Bergen kommune har en **personvernerklæring** elektronisk tilgjengelig for publikum på sine nettsider der det går frem en kortfattet forklaring med definisjoner av relevante begrep. Det går videre klart frem i erklæringen hvilke rettigheter privatpersoner har når det gjelder kommunen sin behandling av deres personopplysninger. Det kommer ikke frem informasjon i undersøkelsen som tyder på at personvernerklæringen ikke er i samsvar med kravene i personvernforordningen artikkel 12 nr. 1.

3.4 Helhetlige føringer for informasjonssikkerhet

3.4.1 Datagrunnlag

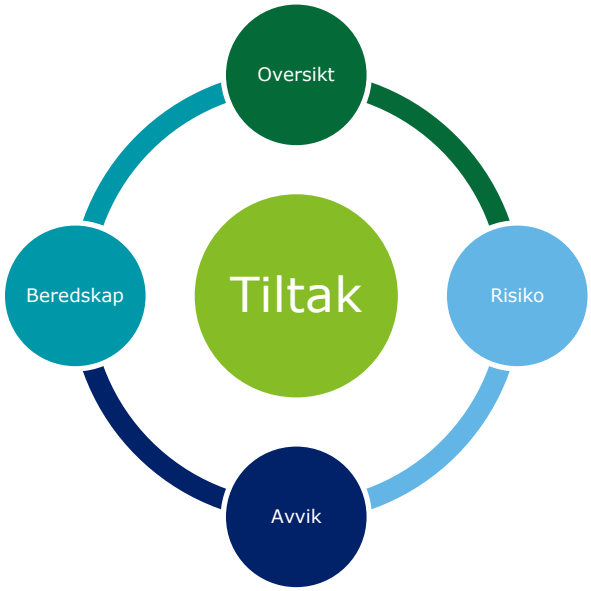
Bergen kommune har utarbeidet føringer for å sikre en felles tilnærming til informasjonssikkerhet i kommunen. Styringssystem, roller og ansvar knyttet til informasjonssikkerhet fremgår i *Reglement for trygg digitalisering*, forskjellige oppdragsbeskrivelser, ulike mandat, samt *Reglement for akseptabel bruk av IKT.* Kommunen har videre utarbeidet veiledere og prosedyrebeskrivelser tilknyttet styringssystemet for personvern og informasjonssikkerhet, samt en rekke beskrivelser og verktøy som er tilgjengelig på kommunens intranett (*Allmenningen*). Alle de ovenfor nevnte dokumentene er tilgjengelig for alle ansatte på *Allmenningen*.

I kommunens *Reglement for trygg digitalisering* blir ansvar og roller knyttet til informasjonssikkerhet beskrevet, samt at det under hver rolle vises til en egen oppdragsbeskrivelse for kommunaldirektør, leder for EDD, resultatenhetsledere og systemeiere (se også kapittel 4). Oppdragsbeskrivelsene bygger på *Modell for trygg digitalisering* (se figur 3) ved at ansvarsoppgavene som blir holdt frem hovedsakelig er basert på de fire hovedpunktene *oversikt*, *risiko*, *avvik* og *beredskap*.[45]

Det fremgår i *Veileder for trygg digitalisering* at *Modell for trygg digitalisering* skal være oppsettet for kommunens systematiske arbeid med informasjonssikkerhet. Modellen er fremstilt i figur 3 under:

[45] Ansvar for opplæring er lagt til i oppdragsbeskrivelse for resultatenhetsleder og kommunaldirektør.

Figur 3: Modell for trygg digitalisering[46]



Som det fremgår av figuren over, er *tiltak* et sentralt element i modell for trygg digitalisering. Dette elementet går ut på at kommunen skal håndtere og dokumentere tiltak etter at *oversikt* er etablert, *risiko* er kartlagt og *avvik* og *beredskap* er håndtert.

I veilederen *Personvern og informasjonssikkerhet for ledere* blir lederoppgaver knyttet til oversikt, risiko, avvik og beredskap presentert. Eksempelvis blir det under punktet *risiko* gjort rede for at dette handler om å «sørge for at enheten jevnlig dokumenterer en systematisk vurdering av risiko for at enhetens egen behandling av informasjon bryter med kommunens sikkerhetsmål». Deretter blir det gitt en kort innledning til det kontekstuelle risikobegrepet før akseptabel risiko, personvernkonsekvensvurdering, risikovurdering og ev. tiltak og oppfølging blir gjennomgått.

Reglement for trygg digitalisering viser også til de ansattes ansvar for å sørge for tilstrekkelig informasjons-sikkerhet. I *Oppdragsbeskrivelsen for alle ansatte for akseptabel bruk av IKT* fremgår det at IKT-utstyr og –systemer skal benyttes i henhold til regler for:

- Informasjonsforvaltning og taushetsplikt
- Brukerkonto, systemtilganger, passord og pin
- Bruk av kommunes IKT-utstyr og –systemer[47]
- Innsyn og systemovervåking

Under hver av disse overskriftene er det punktvis listet opp tilhørende regler, i tillegg til at det under noen av punktene vises til prosedyrer, retningslinjer, sjekkliste og utfyllende informasjon på *Allmenningen*. Det blir i slutten av dokumentet også vist til at IKT Helpdesk skal kontaktes ved behov for assistanse.

Revisjonen har fått tilsendt utkast til internkontrollrapport om SDIs forvaltning av konsernansvaret for informasjonssikkerhet fra 2018.[48] Det blir i rapportutkastet blant annet påpekt at det er svakheter knyttet til logisk oppbygning av intranettsidene og at det burde etableres et meny-punkt som beskriver lederes ansvar og myndighet knyttet til informasjonssikkerhet. Seksjon for internkontroll kommer med flere eksempel på hvordan intranettsidene kan forbedres.

---

[46] Kilde: *Veileder for trygg digitalisering*.
[47] Under denne overskriften er det flere deloverskrifter som tar opp regler for bruk av datamaskin, mobile enheter, internette-post, kalender, fellesområder, eksterne internettbaserte tjenester/lagring («skytjenester») og rutine for forslag til forbedringer og håndtering av avvik.
[48] Utkast rapport: Forvaltning av konsernansvar for informasjonssikkerhet. Byrådsleders avdeling – Seksjon for internkontroll. 25. juni 2018.

På kommunens intranettsider er styringssystemet for personvern og informasjonssikkerhet tilgjengeliggjort, i tillegg til en rekke tilhørende rutinebeskrivelser, veiledere, verktøy o.l. For å få tilgang til dokumentene som utgjør styringssystemet for personvern og informasjonssikkerhet må man fra forsiden på kommunens intranett gå via følgende lenker: 1) *ansatthjelpen*, 2) *virksomhetsstyring, 3) internkontroll* og deretter 4) *informasjonssikkerhet og personvern.* Under den siste overskriften finner man informasjon og dokumentasjon knyttet til tema som vist i figur 4:[49]

Figur 4: Informasjonssikkerhet og personvern på Allmenningen

Under hver av overskriftene finner man nærmere informasjon innenfor området; blant annet er det lagt inn informasjon om systemeiers og resultatenhetsleders ansvar når man går inn på lenken *Roller og ansvar*. Det er ikke lagt inn informasjon om andre roller og ansvar knyttet til informasjonssikkerhet og personvern i kommunen under denne lenken.[50]

Under lenken *Informasjonstjenester og IKT* (som ligger på startsiden til kommunens intranett) kommer man direkte inn på informasjon om blant annet *Helpdesk* og *Systemer, Tilganger og passord.* Under sistnevnte lenke kommer man blant annet til retningslinjene for tilgangsstyring (jf. *Tilgangsstyring*, 3.3.1).

I intervju blir det pekt på at den gjennomgående største utfordringen innenfor informasjonssikkerhet – til liks med de fleste andre tverrsektorielle oppgaver i kommunen – knytter seg til etterlevelsen ute i tjenestene og hos den enkelte ansatte. Det blir opplyst at selv om system, rutiner, retningslinjer og prosedyrer foreligger, kan praksis i kommunens mange enheter være avvikende fra disse på grunn av både kompetanse og kultur (kompetanse og informasjonssikkerhetspraksis i kommunen drøftes i kapittel 5).

Kommunaldirektøren forteller videre at selv om BFIE og SDI kan gi retning, fortolkninger og legge til rette for en god informasjonssikkerhet i kommunen, har de ikke vedtaks- eller instruksjonsmyndighet i andre byrådsavdelinger. De kan derfor heller ikke garantere for at andre byrådsavdelingene fullt ut følger styringssystemet.

Revisjonen får ellers opplyst at det tidligere personvernombudet i kommunen brukte mye tid på å forankre det nye styringssystemet for informasjonssikkerhet hos lederne i kommunen. Videre pekes det på at det i økende grad er klart for den enkelte ansatte hvilket ansvar som påhviler dem med hensyn til informasjonssikkerhet, samtidig som det understrekes at det er en utfordring å nå ut til og etablere en sams forståelse blant alle 18 000 ansatte i kommunen.

[49] Allmenningen.bergen.kommune.no [lest 31.07.2019]. Kommunen har gjort endringer i oppbyggingen av denne intranettsiden i løpet av revisjonsperioden, og noen av endringene samsvarer delvis med seksjon for internkontroll sine anbefalinger fra 2018.
[50] Dette var status per 31. juli 2019.

I spørreundersøkelsen ble respondentene bedt om å oppgi i hvilken grad er det klart for dem hvilket informasjonssikkerhetsansvar som ligger til stillingen deres; langt de fleste svarer enten at det «i svært stor grad» (21 %) eller «i stor grad» (51 %) er klart hvilken informasjonssikkerhetsansvar som ligger til deres stilling; samtidig svarer 30 % av respondentene «nei» på spørsmål om de vet hvor de finner rutiner og retningslinjer for håndtering av personopplysninger, sensitive personopplysninger og/eller annen fortrolig informasjon. Videre svarer rundt halvparten av respondentene at de ikke har lest reglement og veileder for trygg digitalisering, to sentrale dokumenter knyttet til informasjonssikkerhet i kommunen, og over 20 % svarer at de ikke har lest og akseptert *Reglement for akseptabel bruk av IKT*; dette er en obligatorisk øvelse for alle ansatte i kommunen (se også kapittel 5).

3.4.2 Vurdering

Bergen kommune gir gjennom styringssystemet for personvern og informasjonssikkerhet med tilhørende veiledere, prosedyrebeskrivelser, oppdragsbeskrivelser mm. felles føringer for informasjonssikkerhet, og har slik lagt til rette for en helhetlig tilnærming til informasjonssikkerhet i kommunen.

Revisjonen merker seg at svarene i spørreundersøkelsen både indikerer at respondentene opplever sitt informasjonssikkerhetsansvar som tydelig, samtidig som de i relativt liten grad kjenner til hvor de finner relevante rutiner og retningslinjer, og i enda mindre grad har lest og gjort seg kjent med både obligatoriske og sentrale styrende dokumenter. Funn i kapittel 5 kan tyde på at dette delvis har å gjøre med at ikke alle ansatte opplever rutiner og retningslinjer tilhørende styringssystemet som tilstrekkelig tydelige og forståelige, samt at det kan oppleves som vanskelig å orientere seg blant mengden rutiner, retningslinjer, veiledere mm. som foreligger på *Allmenningen*.

Revisjonen registrerer òg at kommunens organisering og størrelse fremholdes som mulige forklaringer på mulig manglende etterlevelse av styringssystemet blant ansatte i enhetene. Uten instruksjonsmyndighet pekes det på at det kan være utfordrende å sikre etterlevelse av styringssystemet for ansvarlig byrådsavdeling.

I sum er det revisjonen sin vurdering at det blir gitt føringer for å sikre en helhetlig tilnærming til informasjonssikkerhet i Bergen kommune, men at det bør iverksettes tiltak for å sikre at styringssystemet faktisk blir etterlevd.

4. Oppgaver og ansvar

4.1 Problemstilling

I dette kapittelet vil vi svare på følgende problemstilling:

I hvilken grad er ansvar og oppgaver knyttet til informasjonssikkerhet tydeliggjort?

4.2 Revisjonskriterier

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.

Med hensyn til roller og ansvar knyttet til personvernsikkerhet, går følgende frem i artikkel 4 nr. 7 og 8 i personvernforordningen:

> 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

I kommunen er det byråden som er behandlingsansvarlig. Databehandlere er eventuelle tjeneste-leverandører 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).

Personvernforordningen pålegger videre kommunen å utpeke et personvernombud, jf. artikkel 37 bokstav a. Artikkel 38 regulerer stillingsvilkårene for personvernombudet, og det går blant annet frem 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 personvern-ombudet 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 personvern-ombudet er bundet av taushetsplikt (nr. 5).

I forvaltningsrevisjonsrapporten fra 2015, anbefalte revisjonen at kommunen gjennomførte følgende tiltak knyttet til systemeierne:

2. Sørge for at systemeiere har tilstrekkelig opplæring og støtteverktøyer for å kunne gjennomføre sine oppgaver.

Se vedlegg 2 for utfyllende revisjonskriterier.

4.3 Ansvar og oppgaver knyttet til informasjonssikkerhet

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 (se også kapittel 3). Ved BFIE, som har konsernansvar for informasjonssikkerhet i kommunen, blir også ansvar tydeliggjort gjennom styrende dokumenter, fullmaktsbrev og avtaler.

Reglement for trygg digitalisering har oversikt over ansvar knyttet til arbeidet med informasjonssikkerhet beskrevet i tabellform (gjengitt i tabell 9):

Tabell 9: Ansvar for informasjonssikkerhet i Bergen kommune

Organisasjonsnivå	Rolle	Beskrivelse
Byrådsavdeling med konsernansvar (BFIE) *Policynivå*	**Kommunaldirektør** **Seksjonsleder digitalisering og innovasjon**	Legge til rette for god praksis i organisasjonen ved å • utarbeide/forvalte konsernsystemer, -rutiner og -verktøy • gi veiledning til byrådsavdelingene • gjennomføre etterkontroller av praksis på utvalgte områder Utarbeide og iverksette overordnet informasjonssikkerhets-strategi Legge til rette for god samhandling mellom konsernfunksjon og byrådsavdelingene når det gjelder informasjonssikkerhet og personvern Legge til rette for ledelsens gjennomgang i alle byrådsavdelinger
Byrådsavdeling med konsernansvar (BFIE) *Driftsnivå*	**Kommunaldirektør** **Seksjonsleder digitalisering og innovasjon** **Leder av Enhet for digitale driftstjenester**	Sørge for at lovens krav til innebygget personvern ivaretas i kommunens IKT-systemer som tilrettelegges og driftes av enheten. Sikre at IKT-systemene tilfredsstiller vedtatte krav til informasjonssikkerhet og personvern
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.

Revisjonen har fått tilsendt fullmaktsbrev som beskriver fullmakter for direktør for SDI delegert fra kommunaldirektør for HR, digitalisering og eiendom per 24. august 2017. I dette fullmaktsbrevet går det frem at kommunaldirektøren på generell basis delegerer sine fagfullmakter på IKT-området til direktør for SDI med noen unntak. Fullmaktsbrevet går videre inn på noen av myndighetsområdene som er tillagt direktør for SDI.

Revisjonen har fått tilsendt *Styrende dokument for digitalisering og IKT i Bergen kommune*.[51] Formålet med dokumentet er å klargjøre organisering, ansvar og roller innenfor digitalisering og IKT i Bergen kommune. Det fremgår videre hvordan digitaliserings- og IKT-området er organisert med utgangspunkt i en bestiller- og utførermodell, der SDI har funksjon som koordinerende bestiller på konsernnivå. SDI skal videre, sammen med EDD, bistå kommunen med å avklare behov, krav og utforming av bestillinger.

Det fremgår i intervju at det er tydelig at det er kommunaldirektør for HR, digitalisering og eiendom som er behandlingsansvarlig for personopplysningene som behandles i BFIE, slik som kommunaldirektørene i de andre byrådsavdelingene er behandlingsansvarlig for personopplysningene som behandles der. I tillegg har kommunaldirektør for HR, digitalisering og eiendom det overordnede informasjonssikkerhetsansvaret i kommunen, inkludert for styringssystemet for informasjonssikkerhet. Videre blir det fortalt at kommunaldirektør for HR, digitalisering og eiendom har et aktivt ledelsesansvar for det revitaliserte informasjonssikkerhetsforumet som ble startet opp igjen ved implementeringen av det nye styrings-systemet for personvern og informasjonssikkerhet høsten 2018.

Det blir videre fortalt i intervju at kommunaldirektør for HR, digitalisering og eiendom har godkjenningsansvar for styringssystemet for informasjonssikkerhet, noe som i praksis innebærer at systemet i stor grad er utarbeidet av direktøren for SDI, ved hjelp av innspill og høringsuttalelser fra ulike instanser, men at det først er gjeldende når kommunaldirektør for HR, digitalisering og eiendom har godkjent det. Det fremgår videre i intervju at direktør for SDI kan videredelegere myndighet i egen seksjon, men selv beholder ansvaret.

Revisjonen får opplyst at det p.t. i praksis er direktør for SDI som er informasjonssikkerhetsansvarlig på SDI.[52] Det fremgår videre i intervju at det er flere informasjonssikkerhetsrådgivere som bistår seksjonen med informasjonssikkerhetsoppgaver.

Det understrekes i intervju at Bergen kommune er et konglomerat av ulike virksomheter, med en styrings-modell og et politisk system som sprer ansvaret og myndigheten mellom byrådsavdelingene. Det fremholdes videre at kommunens størrelsen, det vide spekteret av tjenester, og den parlamentariske styringsmodellen, samlet fører til at det kan være utfordrende å ha full oversikt over praksis i alle avdelinger og tjenester innenfor de tverrgående ansvarsområdene som ligger til kommunaldirektør for HR, digitalisering og eiendom (se også seksjon 3.4).

Samtidig blir det nevnt i intervju at det blir arbeidet godt med å avklare byrådsansvar når ansvar ligger på tvers av avdelingene. I denne sammenheng blir det vist til drøftinger mellom BBSI og BFIE knyttet til en alvorlig informasjonssikkerhetshendelse i 2018 som var knyttet til begge avdelinger.

Det blir fortalt i intervju at det ikke er grunn til å tro at noen i kommunen bestrider at informasjonssikkerhet og styringssystem ligger under BFIE/SDI sitt ansvarsområde, men at det likevel finnes gråsoner det er viktig å ha fokus på. Som eksempel på slike gråsoner nevnes overgangene mellom helse og omsorg sitt behandlingsansvar og eierskap for sine system og EDD som drifter nettverk, sikker sone og øvrig infra-struktur.

Oppgaver og roller knyttet til informasjonssikkerhet i kommunen

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 resultat-enhetsledere 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 10:

[51] Styrende dokument for digitalisering og IKT i Bergen kommune. Organisering, roller og ansvar. Revisjonsdato 15.10.2018. Gyldig til 01.12.2020.
[52] Det blir opplyst i intervju (4. april 2019) at det er pågående rekrutteringsprosesser for å få plass ny funksjon som informasjonssikkerhetsansvarlig.

Tabell 10: 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 informasjonssikkerhetsforum 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 egenresultatenhet.
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 for eksempel systemkoordinator eller IKT-koordinator i *Reglement for trygg digitalisering*.

Utkastet til internkontrollrapporten av SDIs forvaltning av konsernansvaret for informasjonssikkerhet[53] viser til at det er utfordringer knyttet til oppfølgingen av informasjonssikkerhet i kommunen. I følge rapporten er manglende tilrettelegging fra BFIE en viktig årsak til at det er utfordringer med å få aktører i kommunen til å forstå og ta ansvar for sine roller innenfor fagområdet.

[53] Utkast rapport: Forvaltning av konsernansvar for informasjonssikkerhet. Byrådsleders avdeling – Seksjon for internkontroll. 25. juni 2018.

Behandlingsansvarlige

Som vist i tabell 10 fremgår det av *Reglement for trygg digitalisering* at det er kommunaldirektørene i kommunen som har rollen som behandlingsansvarlig. Med dette har de ansvar for å sørge for at personvernregelverket etterleves i egen virksomhet, og de skal videre følge opp at ledere, systemeiere og ansatte følger sine respektive oppdragsbeskrivelser.

I oppdragsbeskrivelsen for kommunaldirektør[54] går følgende ansvarsområder med tilhørende oppgavebeskrivelser frem:

- Personvern og informasjonssikkerhet i egen byrådsavdeling
- Oversikt over behandling av personopplysninger
- Risikostyring av personvern og informasjonssikkerhet
- Avvik i forbindelse med personvern og informasjonssikkerhet
- Beredskap i forbindelse med personvern og informasjonssikkerhet
- Opplæring i personvern og informasjonssikkerhet

Som en del av sitt ansvar knyttet til informasjonssikkerhet, skal kommunaldirektørene delta i informasjonssikkerhetsforum. I *Mandat for informasjonssikkerhetsforum* blir det slått fast at kommunaldirektørene skal delta selv eller med en representant i forumets møter. I intervju blir det fortalt at kommunaldirektørene ikke alltid deltar med egnede representanter i informasjonssikkerhetsforum, men sender representanter uten tilstrekkelig myndighet. Det blir videre fortalt at det er leder for informasjonssikkerhetsforum, kommunaldirektør for HR, digitalisering og eiendom, som har ansvar for å gi tilbakemelding om dette til vedkommende kommunaldirektør.

Personvernombud

Som vist i tabell 10 blir det i *Reglement for trygg digitalisering* vist til personvernombudets overordnete oppgaver og ansvar knyttet til personvern og informasjonssikkerhet. Personvernombudets ansvar og rolle i kommunen er videre utdypet i *Mandat for Personvernombudet*.

I sistnevnte dokument[55] fremgår hovedoppgaver, kvalifikasjoner og myndighet i rollen som personvernombud, og det blir beskrevet at personvernombudet er uavhengig i sin rolle og at vedkommende skal rapportere jevnlig og direkte til øverste ledelse i kommunen. For øvrig beskrives oppgaver og bidrag knyttet til rådgivning, kunnskapsformidling, overordnet styrings- og internkontrollsystem, samarbeid, informasjonsoversikt, kontaktpunkt, beredskap, revisjon, avvikshåndtering og vurdering av risiko og personvernkonsekvenser.

I intervju med forhenværende konstituert personvernombud[56] blir det fortalt at personvernombudets ansvar blir oppfattet som tydelig beskrevet i mandatet. Videre blir det fortalt at det er en tydelig rolle- og ansvarsdeling mellom rådgiverne på avdeling for personvern og informasjonssikkerhet. Dette til tross for at rolle- og ansvarsfordelingen ikke er formalisert. Det blir videre fortalt at oppgavene fordeles etter kompetanse, erfaring og kapasitet og at de ansatte på avdelingen over tid har fått egne «ekspertfelt» og kundeporteføljer, som styrer videre fordeling av ansvar og oppgaver blant rådgiverne.

Videre blir det fortalt i intervju at personvernombudet rapporterer direkte til kommunaldirektøren og ikke direktør for SDI, og at dette er for å skape et tydelig skille som viser personvernombudets uavhengig rolle.

Det fremgår av intervju at måten personvernombudet er organisert på opp mot SDI og EDD på sikt skal evalueres. Det blir fortalt at det kan oppstå utfordringer ved at personvernombudet ligger organisert i linjen, men at det samtidig ikke er ønskelig å organisere personvernombudet på utsiden av avdelingen.[57]

---

[54] Oppdrag – personvern og informasjonssikkerhet for kommunaldirektør. Revisjonsdato 05.09.2018. Gyldig til 13.09.2019.
[55] Mandat for personvernombud. Revisjonsdato 29.08.2018. Gyldig til 13.09.2019.
[56] Vedkommende var konstituert personvernombud fra 1. januar 2019 til 1. april 2019.
[57] Seksjon for internkontroll i Bergen kommune gir i utkast til internkontrollrapport av forvaltning av konsernansvar for informasjonssikkerhet anbefaling om at «BFIE gjør en vurdering om dagens organisering av personvernombudsordningen i Bergen kommune er hensiktsmessig for å sikre en tydelig, og uavhengig, stemme i arbeidet med personvernet» (s. 30).

I forbindelse med verifiseringen av rapporten opplyses det at organiseringen av personvernombudet har blitt diskutert med Datatilsynet, og at det ikke har fremkommet innvendinger mot dagens organisering. Videre kommer det frem at personvernombudet opplever god kontakt med ledelse og ansvarlige i Bergen kommune.

Resultatenhetsleder

I *Reglement for trygg digitalisering* går resultatenhetsleders ansvar, rolle og oppgaver knyttet til informasjonssikkerhet og personvern frem (se tabell 9 og tabell 10). Under oppgavebeskrivelsen blir det vist til *Oppdrag – personvern og informasjonssikkerhet for resultatenhetsledere*[58] med lenke til dokumentet på *Allmenningen*.

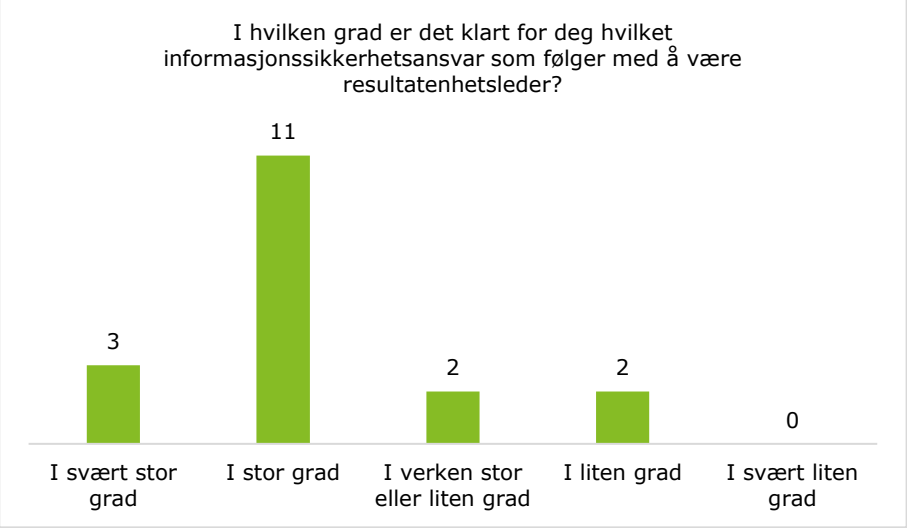
I oppdragsbeskrivelsen fremgår det hvilke oppgaver resultatenhetsleders er ansvarlig for at blir etterlevd knyttet til oversikt, risiko, avvik, beredskap og opplæring. Blant annet er resultatenhetsleder ansvarlig for at enheten fører en dokumentert oversikt over hvilken informasjon den behandler, hvor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

Av de totalt 18 respondentene som oppgir i spørreundersøkelsen at de er resultatenhetsledere, svarer syv at de ikke har lest *Oppdragsbeskrivelsen for resultatenhetsledere knyttet til personvern og informasjons-sikkerhet*, syv svarer at de har leste den, mens fire ikke vet om de har lest den.

Resultatenhetslederne i spørreundersøkelsen fikk også spørsmål om de har lest *Veileder – personvern og informasjonssikkerhet for ledere*. På dette spørsmålet svarer åtte «ja», seks «nei» og fire «vet ikke».

På spørsmål om de opplever ansvaret til resultatenhetsledere knyttet til informasjonssikkerhet som tydelig, fordeler svarene til de 18 resultatenhetslederne seg som vist i figur 5 under:

Figur 5: Tydelig informasjonssikkerhetsansvar for resultatenhetsleder

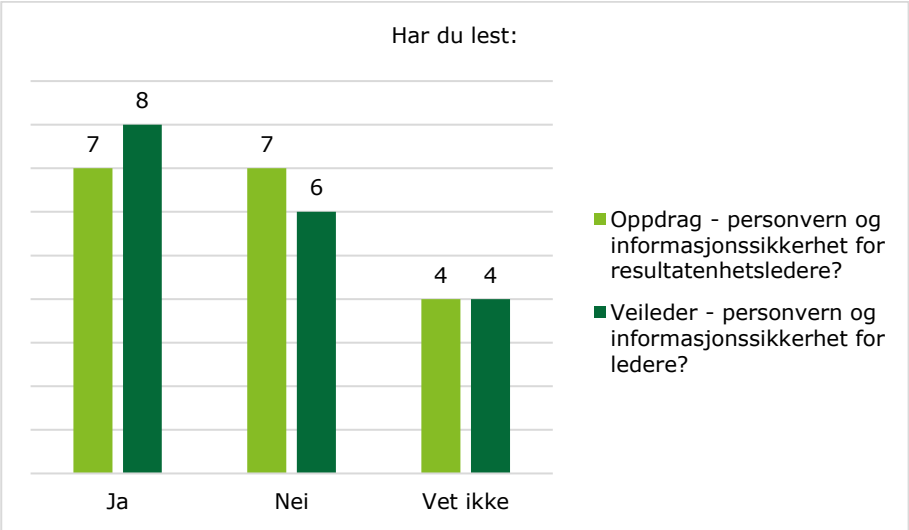


Av figuren fremgår det at til sammen 14 av resultatenhetslederne i spørreundersøkelsen mener at informasjonssikkerhetsansvaret «i svært stor grad» eller «i stor grad» er klart, mens to svarer at det «i verken stor eller liten grad» er klart, og de siste to at det «i liten grad er» er klart.

Resultatenhetsledere fikk også spørsmål om de har lest *Oppdrag – personvern og informasjonssikkerhet for resultatenhetsledere* og *Veileder – personvern og informasjonssikkerhet for ledere* (se figur 6):

[58] Oppdrag – personvern og informasjonssikkerhet for resultatenhetsledere. Ikke datert.

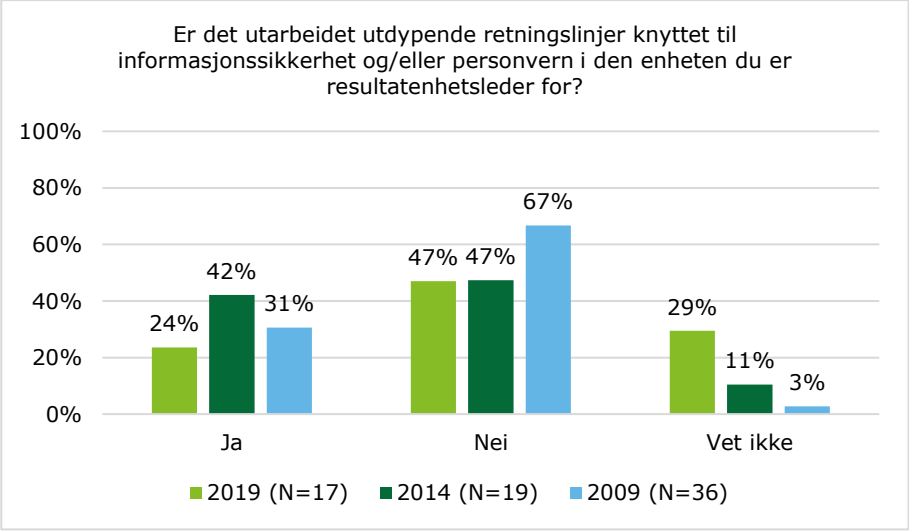
Figur 6: Kjennskap til sentrale dokument (resultatenhetsledere)[59]



Som vist i figuren svarer like mange resultatenhetsledere (7) at de *har* som at de *ikke har* lest oppdragsbeskrivelsen, mens to flere (8) svarer at de har lest veilederen enn som svarer at de ikke har det (6). 4 av 18 resultatenhetsledere svarer «vet ikke» både på spørsmål om de har lest oppdragsbeskrivelsen og om de har lest veilederen.

I spørreundersøkelsen ble resultatenhetslederne spurt om det er «utarbeidet utdypende retningslinjer knyttet til informasjonssikkerhet og/eller personvern» i enheten de er leder for. Også i spørre-undersøkelsene i 2014 og 2009 ble resultatenhetslederne stilt dette spørsmålet. Svarene fra de tre spørre-undersøkelsene er gjengitt i figuren under:

Figur 7: Utfyllende retningslinjer for informasjonssikkerhet

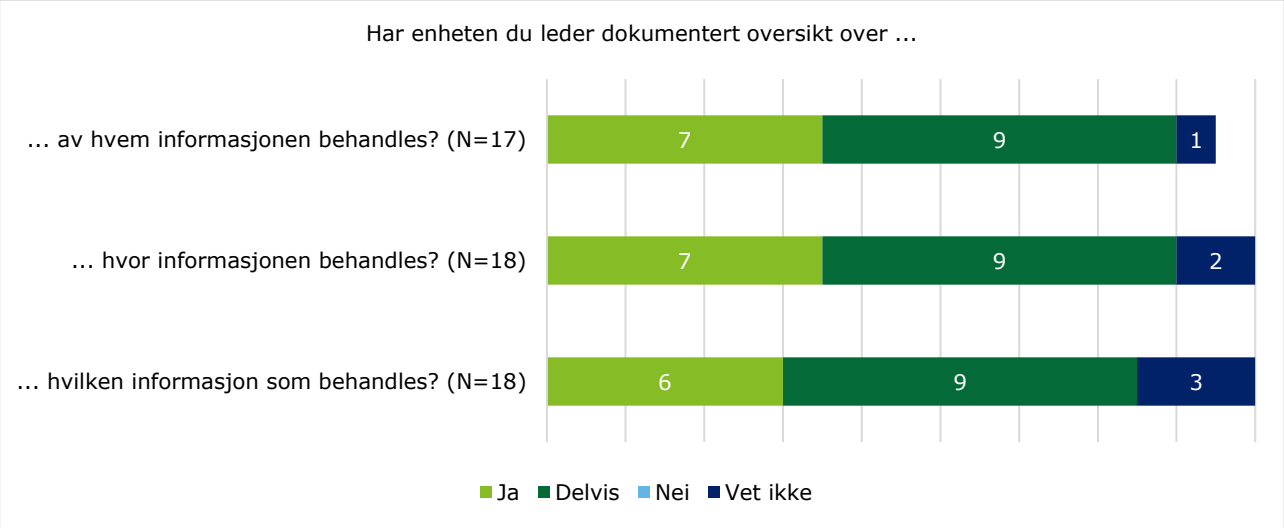


Som det går frem av figur 7, svarer en lavere andel av enhetslederne «ja» på spørsmålet i 2019 enn i de foregående årene, mens en høyere andel svarer «vet ikke».

Resultatenhetslederne fikk videre spørsmål om de som leder har dokumentert oversikt over hvilken informasjon som behandles på enheten, hvor informasjonen behandles og av hvem informasjonen behandles:

[59] N=18.

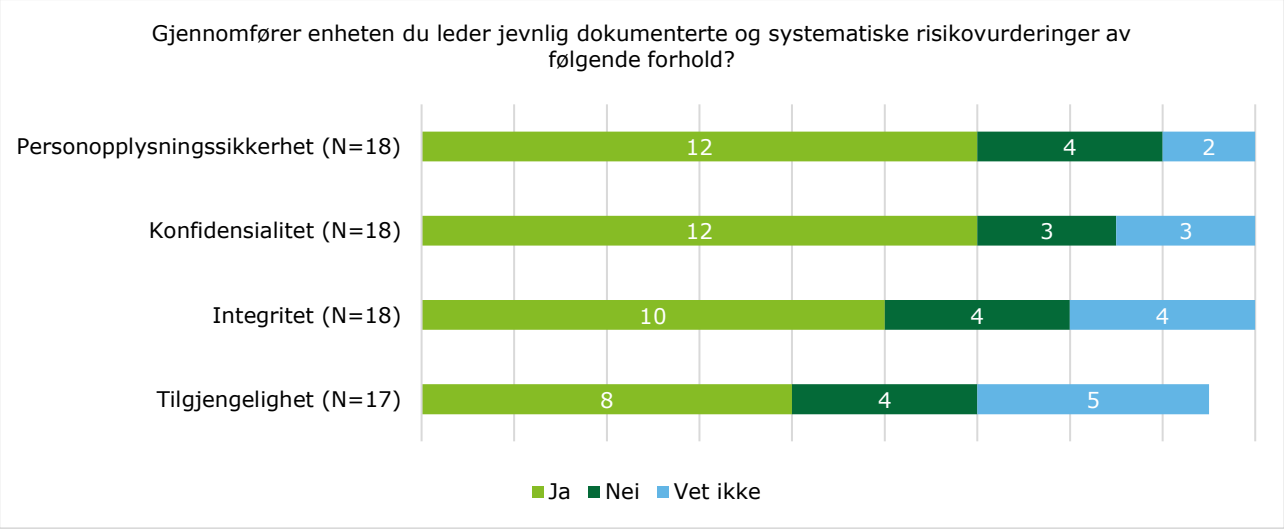
Figur 8: Resultatenhetsleder: dokumentert oversikt over behandling av informasjon



Som fremstilt i figur 8 over svarer mellom én og tre av resultatenhetslederne «vet ikke» på de tre spørsmålene, ni svarer «delvis» på spørsmålene, mens mellom seks og syv svarer «ja». Ingen svarer «nei».

Resultatenhetslederne i spørreundersøkelsene fikk også spørsmål om hvorvidt enheten gjennomfører «jevnlig dokumenterte og systematiske risikovurderinger» av forhold knyttet til personopplysnings-sikkerhet,[60] konfidensialitet,[61] integritet[62] og tilgjengelighet.[63] Svarene er fremstilt i figuren under:

Figur 9: Dokumentasjon og systematiske risikovurderinger



Mellom tre og fire av resultatenhetslederne svarer at enheten de leder *ikke* gjennomfører «jevnlig dokumenterte og systematiske risikovurderinger av personopplysningssikkerhet, integritet og tilgjengelighet». Tilsvarende svarer mellom to og fem «vet ikke» på spørsmålene, mens mellom åtte og 12 svarer «ja».

Respondentene som svarte «nei» på disse spørsmålene, fikk oppfølgingsspørsmål om hva som er bakgrunnen for at disse risikovurderingene ikke blir utført.[64] Gjennomgående svarte de fleste at de «ikke

[60] At enheten ivaretar personvernet til ansatte og innbyggere i sin informasjonsbehandling
[61] At uvedkommende ikke får tilgang til informasjon som følge av enhetens informasjonsbehandling
[62] At det ikke oppstår feil eller mangler i informasjonen enheten behandler eller er avhengig av
[63] At informasjonen enheten behandler eller er avhengig av ikke blir utilgjengelig
[64] Det var mulig for respondentene å krysse av for flere alternativer

har vært klar over at det er forventet at dette skal gjøres», mens resten svarte de «ikke har hatt tid til å gjøre det». Ingen av respondentene viste til manglende kompetanse eller manglende tilgang på verktøy som årsak til manglende risikovurderinger.

Systemeier

Reglement for trygg digitalisering viser til systemeiers rolle og oppgaver når det gjelder informasjonssikkerhet og personvern (se tabell 10). Under oppgavebeskrivelsen blir det henvist til *Oppdrag – personvern og informasjonssikkerhet for systemeiere* med lenke til oppdragsbeskrivelsen på *Allmenningen*.

I oppdragsbeskrivelsen 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 personvernkonsekvensvurdering og teknisk risikovurdering.

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

Tabell 11: 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 tilsendt en oversikt over systemeiere i Bergen kommune. Her er det lagt inn 330 system[65] fordelt på 74 systemeiere:

[65] I en av radene er det ikke fylt ut navn på system.

Tabell 12: Oversikt over systemeiere[66]

Avdeling	Antall systemeiere
BBSI	11 systemeiere
BBU	9 systemeiere
BFIE	20 systemeiere[67]
BHO	11 systemeiere
BKKN	4 systemeiere[68]
BLED	9 systemeiere
BORG[69]	1 systemeier
BSBI	9 systemeiere
Bergen Vann KF	1 systemeier

Respondentene i spørreundersøkelsen fikk spørsmål om de er systemeiere. Totalt svarte om lag 10 % «vet ikke» på spørsmålet, mens rundt 89 % svarer «nei» og i overkant av 1 % «ja».[70] De fem som svarte at de er systemeiere, fikk oppfølgingsspørsmål om hvorvidt de opplever at det er et klart informasjons-sikkerhetsansvar som følger med rollen. Alle fem svarte at dette enten «i stor grad» eller «i svært stor grad» er tydelig.[71]

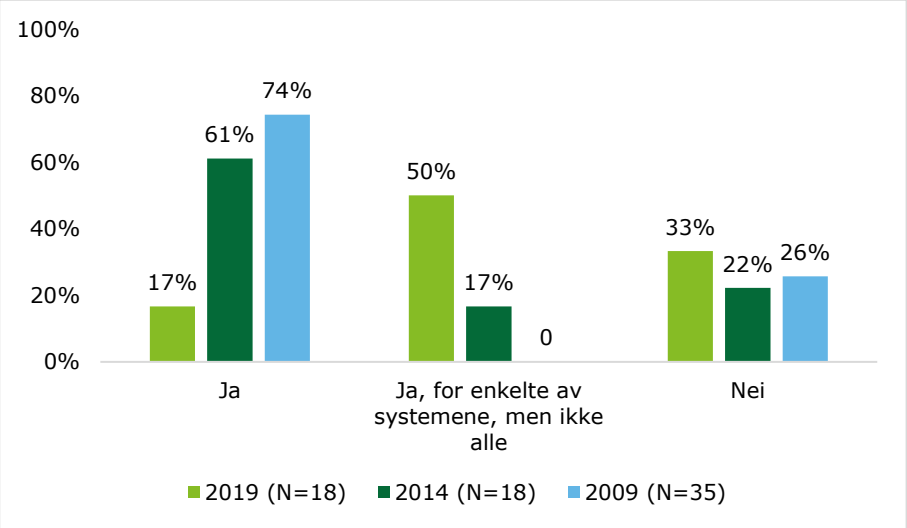
De samme respondentene fikk videre spørsmål om de har lest *Oppdragsbeskrivelse for systemeiere knyttet til personvern og informasjonssikkerhet*. På dette spørsmålet svarte de fleste «nei».

Systemeierne fikk også spørsmål om de har sikret at systemene de eier er 1) meldt til kommunens personvernombud, 2) er sikret i henhold til sjekkliste for grunnsikring av IKT-systemer i Bergen kommune og 3) om personvernkonsekvensvurdering og teknisk risikovurdering er gjennomført, oppdatert og dokumentert på systemets offisielle saksnummer. På de to første delspørsmålene svarte de fleste «ja», men ikke alle visste om dette var gjort. På det siste delspørsmålet kom det både «ja», «nei» og «vet ikke»-svar.

De respondentene som oppgir at de er resultatenhetsledere i spørreundersøkelsene gjennomført i 2019, 2014 og i 2009 fikk spørsmål om de vet «hvem som er systemeiere av systemene som benyttes i din resultatenhet». Svarene fra resultatenhetslederne for de tre årene er fremstilt i figur 10 under:

[66] Noen systemeiere har ansvar for flere byrådsavdelinger og dermed blir ikke antall systemeiere i tabellen og samlet antall systemeiere det samme.
[67] Flere av systemene registrert på BFIE brukes i flere byrådsavdelinger. Elevarkivet i BK360 har ennå ikke fastsatt systemeier. Revisjonen registrerer at forhenværende Personvernombud er registrert som systemeier for *junglemaps*.
[68] Ett av systemene, ticket.co, står som merket som «uavklart» når det gjelder systemeier.
[69] Inkludert bystyrets kontor
[70] N=380
[71] N=5

Figur 10: Vet du hvem som er systemeiere av systemene som benyttes i din resultatenhet?[72]



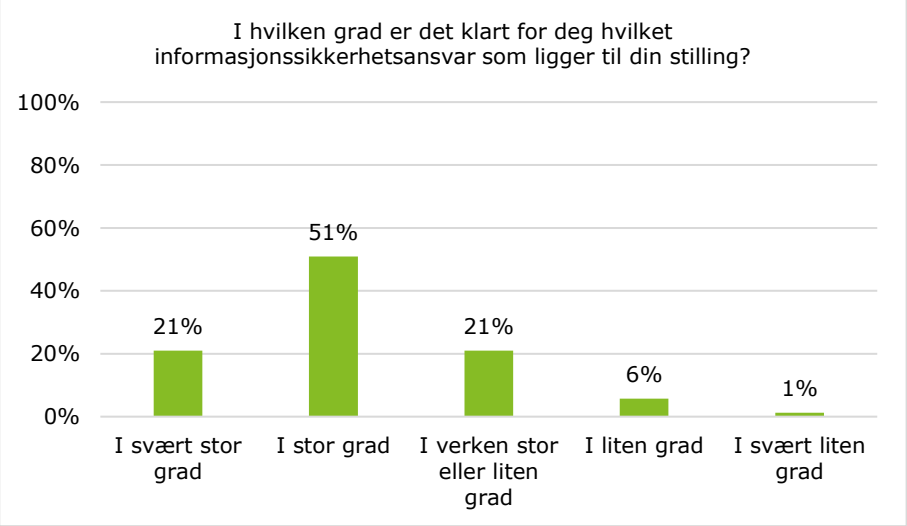
Som vist i figur 10, svarer en langt lavere andel «ja» på spørsmålet i 2019 enn i 2014 og 2009. Tilsvarende svarer en noe høyere andel av enhetslederne i 2019 «nei» enn i 2014 og 2009, og endelig svarer halvparten av enhetslederne i 2019 at de ikke vet hvem som er systemeier for alle systemene som benyttes i enheten. I 2014 svarte 17 % det samme.

Ansatte

Som nevnt i avsnitt 3.4.1, viser *Reglement for trygg digitalisering* til de ansattes informasjonssikkerhets-ansvar, mens det i *Oppdragsbeskrivelsen for alle ansatte for akseptabel bruk av IKT* 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*.

Respondentene som svarte at de ikke er resultatenhetsleder eller systemeier ble i spørreundersøkelsen spurt om i hvilken grad det er klart hvilket informasjonssikkerhetsansvar som ligger til deres stilling. Svarene er gjengitt i figur 11:

Figur 11: Stillingens informasjonssikkerhetsansvar (N=314)



Som det fremgår av figuren over, svarer langt de fleste enten at det «i svært stor grad» (21 %) eller «i stor grad» (51 %) er klart hvilket informasjonssikkerhetsansvar som ligger til stillingen; rundt én av fem svarer at det «i verken stor eller liten grad» er klart, mens en relativt lav andel av respondentene svarer

[72] I undersøkelsen som var gjort i 2009 var «ja»/nei» eneste svaralternativ

at det «i liten grad» (6 %) eller «i svært liten grad» (1 %) er klart. Ansattes kjennskap til rutiner og retningslinjer blir videre drøftet i kapittel 5.

Databehandlere og databehandleravtaler

Det fremgår ikke eksplisitt fra tilsendt dokumentasjon hvem som er ansvarlig for å holde og ajourføre oversikten over databehandlere og databehandleravtaler.

Fra tilsendt oversikt over kartlegging av behandlinger av personopplysninger i systemet BK Prosjekt, går det frem at det er 321 databehandleravtaler for de 347 kjente systemene der det behandles personopplysninger. Revisjonen har òg fått tilsendt en forenklet oversikt over databehandleravtaler i kommunen.[73] I dokumentet er det lagt inn informasjon om 351 system, og for 64 av dem fremgår det at de er «ferdig dokumentert» når det gjelder databehandleravtaler. Under kolonnen «databehandleravtaler» er videre 18 system merket med «ikke utarbeidet», 31 som «under arbeid», 197 som «ikke nødvendig», ett som «ikke meldt», 22 som «utarbeidet» og for 13 system er det ikke lagt inn informasjon om status på databehandleravtaler.[74]

Forhenværende konstituert personvernombud opplyser at det er systemeier eller systemkoordinator som melder inn til personvernombudet hvilke system som benyttes, og i den videre dialogen har man kartlagt om det foreligger databehandleravtaler eller ikke. Personvernombudet legger deretter oversikten manuelt inn i sak/arkiv-systemet. Det fremgår videre at personvernombudet jevnlig korrigerer for feilkilder ved at de sender sine oversikter til byrådsavdelingene for verifisering og tilbakemelding.

Ifølge forhenværende konstituert personvernombud er det trolig inngått flere databehandleravtaler enn det som er registrert hos personvernombudet, og at kommunen følgelig ikke har fullstendig oversikt over inngåtte databehandleravtaler.

I forbindelse med verifiseringen av rapporten blir det påpekt at oversikt over databehandlere og databehandleravtaler delvis blir ivaretatt av avdeling for personvern og informasjonssikkerhet ved at det er stilt krav om *Melding om behandling av personopplysninger*.[75] Slike meldinger danner grunnlag for føring av protokoll, hvor også databehandlere og databehandleravtaler skal fremkomme.

4.4 Vurdering

Gjennom styringssystemet for personvern og informasjonssikkerhet og tilhørende oppdragsbeskrivelser, mandater og veiledere, har Bergen kommune skriftliggjort ansvar og oppgaver knyttet til informasjonssikkerhet. Konsernansvaret for informasjonssikkerhet er tydelig lagt til BFIE, og det foreligger fullmakter og avtaler som plasserer ansvar og oppgaver nedover i byrådsavdelingen. I de ulike dokumentene fremgår det videre 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, rollen til informasjonssikkerhetsforum fremgår, og både ansvaret og de respektive oppgavene til resultatenhetsledere, systemeiere og ansatte er skriftliggjort.

Også rollen og ansvaret til personvernombudet er definert skriftlig; dette er en lovregulert rolle, og basert på det som kommer frem i undersøkelsen har ikke revisjonen informasjon som tyder på at mandatet til stillingen ikke oppfyller kravene i artikkel 39 i personvernforordningen.

Det går imidlertid ikke frem i undersøkelsen hvem som er ansvarlig for å holde og ajourføre oversikten over databehandlere og databehandleravtaler. Revisjonen registrerer at dette ansvaret delvis er ivaretatt av avdeling for personvern og informasjonssikkerhet gjennom prosedyrene knyttet til melding om

---

[73] Gjennom intervju med forhenværende konstituert Personvernombud blir det fortalt at den forenklede oversikten over databehandleravtaler som revisjonen har fått tilsendt er et resultat av innmelding av system til Personvernombudet fra byrådsavdelingene.

[74] I regnearket som utgjør den forenklete oversikt over databehandleravtaler er det et ark med oversikt over systemer for test og utvikling, der det er lagt inn 43 system: knyttet til databehandleravtaler er to registrert som «ferdig dokumentert», tre som «under arbeid», én som «ikke utarbeidet», 19 som «ikke nødvendig» og for 17 system er det ikke lagt inn informasjon.

[75] Se avsnittet *Oversikt over personopplysninger* på side 16.

behandling av personopplysninger. Likevel merker revisjonen seg at kommunen etter eget utsagn ikke har full oversikt over inngåtte databehandleravtaler.

Selv om både systemeierne og resultatenhetslederne som svarte på undersøkelsen i hovedsak oppgir at deres eget informasjonssikkerhetsansvar er tydelig, viser svarene på andre spørsmål i spørreundersøkelsen at ansvaret og oppgavene ikke er tilstrekkelig kjent. Sett i sammenheng med funnene i kapittel 5 knyttet til respondentenes kjennskap til og etterlevelse av kommunens gjeldende regelverk, rutiner, veiledere, prosedyrer mm. for informasjonssikkerhet, er det revisjonen sin vurdering at Bergen kommune ikke i tilstrekkelig grad har tydeliggjort ansvar og oppgaver knyttet til informasjonssikkerhet.

Svarene i spørreundersøkelsen tyder òg på at kommunen ikke i tilstrekkelig grad har sørget for at «systemeiere har tilstrekkelig opplæring og støtteverktøyer for å kunne gjennomføre sine oppgaver», og slik ikke fulgt opp denne anbefalingen fra revisjonen i 2015.

Basert på funnene i undersøkelsen, er det revisjonens vurdering at Bergen kommune ikke fullt ut oppfyller kravet i ISO275001, kapittel 5.3, om at den «øverste ledelsen skal sikre at ansvar og myndighet for roller som er relevante for informasjonssikkerheten, er tildelt og kommunisert».

Revisjonen registrerer at blant annet kommunens størrelsen og den parlamentariske styringsmodellen i Bergen fremholdes som medvirkende årsaker til at det kan være utfordrende for BFIE ved SDI å fullt ut sikre at de enkelte byrådsavdelinger ivaretar sitt ansvar for informasjonssikkerhet. Revisjonen mener at det er etablert et overordnet styringssystem for informasjonssikkerhet, men revisjonen vil understreke viktigheten av at den enkelte byrådsavdeling i kommunen følger opp sitt ansvar for å etterleve dette styringssystemet, for eksempel ved å sikre at deres representant i informasjonssikkerhetsforum har tilstrekkelig myndighet.

Revisjonen er videre oppmerksom på at det er relativt kort tid siden gjeldende styringssystem for personvern og informasjonssikkerhet ble utarbeidet og implementert i kommunen, men vil likevel understreke viktigheten av å gjøre styringssystemet og tilhørende reglement, oppdragsbeskrivelser mm. kjent blant de ansatte i kommunen.

5. Kompetanse blant de ansatte

5.1 Problemstilling

I dette kapittelet vil vi svare på følgende problemstilling:

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

5.2 Revisjonskriterier

Kommunen er gjennom eForvaltningsforskriften § 15 forpliktet å ha en internkontroll basert på anerkjente standarder for styringssystem for informasjonssikkerhet. Departementet har utpekt 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.

Datatilsynet sin veileder *Internkontroll og informasjonssikkerhet*[76] omhandler blant annet oppfølging og opplæring. Her går det frem 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. Brukerne 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.

I forvaltningsrevisjonsrapporten fra 2015, anbefalte revisjonen at kommunen gjennomførte følgende tiltak knyttet til kompetanse og opplæring:

3. Sørge for at retningslinjer og rutiner på informasjonssikkerhet er oppdatert og sikre at alle ansatte kjenner til hvor man finner rutinene.

Se vedlegg 2 for utfyllende revisjonskriterier.

5.3 Kjennskap til retningslinjer og rutiner for informasjonssikkerhet blant ansatte

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.

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

Kommunen opplyser at SDI gjennomfører overordnet opplæring for ansatte i kommunen knyttet til informasjonssikkerhet og personvern. Alle nyansatte skal ifølge kommunen gjennomføre KS-læringskurset «nyansatt i Bergen kommune» som inneholder et avsnitt om informasjonssikkerhet. I tillegg blir ansatte tilbudt flere nettbaserte kurs.[77] Det vises videre til at det under nasjonal sikkerhetsmåned (oktober) i 2016 og 2017 ble sendt ut ett slikt kurs i uken til alle ansatte. Dette ble ikke gjennomført i 2018.

Revisjonen får opplyst at alle ledere i kommunen må gjennomføre *Basiskurs for ledere* der blant annet informasjonssikkerhet inngår som tema. Videre nevnes det at kurs for ledere knyttet til informasjonssikkerhet og personvern er under utarbeidelse og planlegges gjennomført i løpet av høsten 2019.

Utenom kursene nevnt ovenfor blir intranettet brukt til å informere ansatte om informasjonssikkerhet; dette skjer både gjennom styrende dokumenter, foreliggende rutiner, retningslinjer og prosedyrer, samt tilgjengelige *oppgaveløsere*[78] og relevante nyhetssaker som ved anledning blir lagt ut på nyhetsstrømmen.

Avdeling for personvern og informasjonssikkerhet har gjennomført over 100 presentasjoner om informasjonssikkerhet for ulike avdelinger i kommunen de siste tre årene. I tillegg viser kommunen til at det foregår læring gjennom samarbeidet mellom avdeling for personvern og informasjonssikkerhet og resultatenhetene.

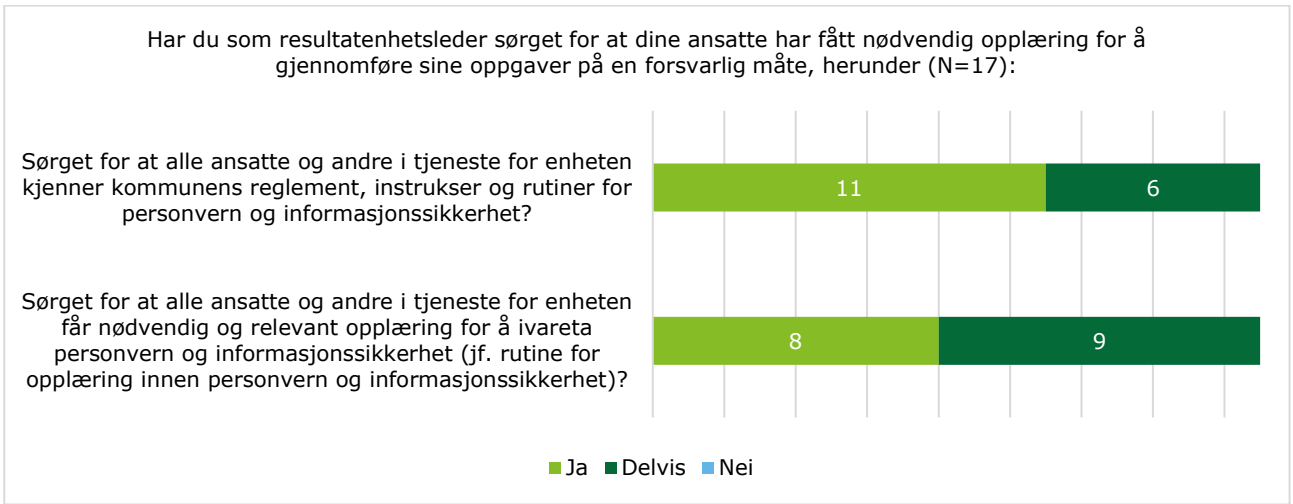
Ansvaret for å sørge for kompetanse innenfor informasjonssikkerhet blant ansatte er gjennom *Reglement for trygg digitalisering* og *Oppdragsbeskrivelse for resultatenhetsledere* plassert hos resultatenhetslederne i kommunen. I oppdragsbeskrivelsen fremgår det at lederens ansvar er å:

- 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*.[79]

Resultatenhetslederne som besvarte spørreundersøkelsen fikk spørsmål om hvorvidt de har sørget for at deres ansatte har fått nødvendig opplæring innenfor informasjonssikkerhetsområdet (se figur 12):

Figur 12: Besørget opplæring

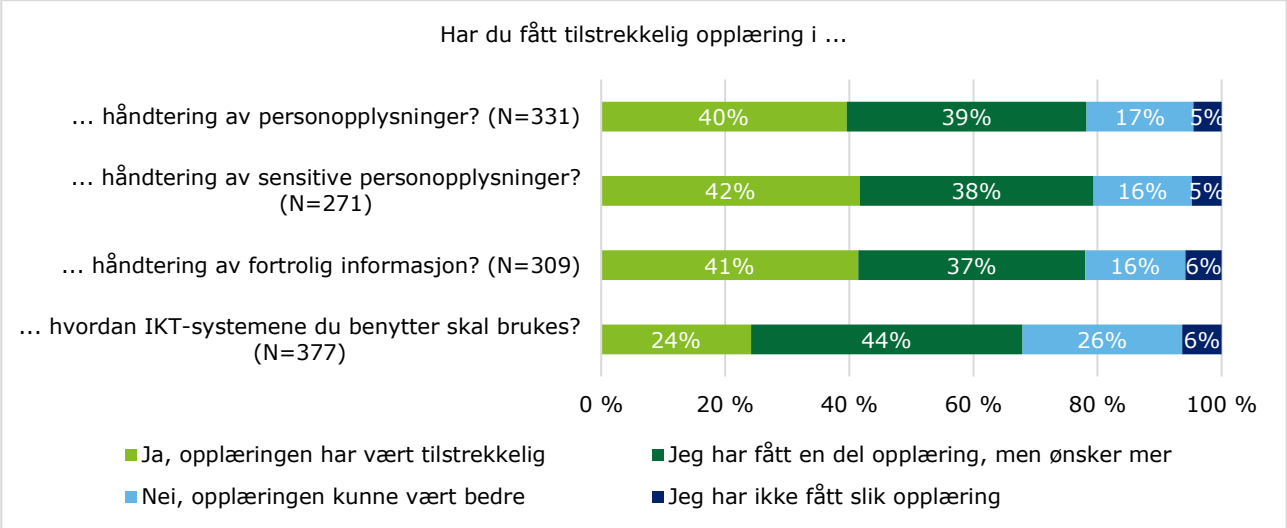


[77] Revisjonen har fått tilsendt en oversikt som viser at det er gjennomført 21 slike nettbasert kurs siden 2016.
[78] Det er tilgjengelige oppgaveløsere på intranettet for alle ansatte i kommunen. Disse er hovedsakelig «bruksanvisninger» for hvordan å utføre oppgaver, og noen av dem er knyttet til informasjonssikkerhet og personvern.
[79] 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».

Som fremstilt i figuren over svarer henholdsvis elleve og åtte av resultatenhetslederne «ja» på de to delspørsmålene, mens seks og ni svarer «delvis». Ingen svarer «nei».

Deltakerne i spørreundersøkelsen fikk spørsmål om hvorvidt de opplever å ha fått tilstrekkelig opplæring i håndtering av ulike typer personopplysninger og fortrolig informasjon og bruk av IKT-systemer:

Figur 13: Mottatt opplæring



Som fremstilt i figur 13 svarer 5-6 % av respondentene at de ikke har fått opplæring i håndtering av fortrolig informasjon, sensitive personopplysninger eller personopplysninger. 16-17 % av respondentene svarer at opplæringen kunne vært bedre på de tre områdene, mens 37-39 % oppgir at de har fått en del opplæring knyttet til håndtering av fortrolig informasjon, personopplysninger og sensitive person-opplysninger, men ønsker mer. Videre svarer 6 % av respondentene at de ikke har fått opplæring i hvordan IKT-systemene de benytter skal brukes, og på samme spørsmål svarer 26 % «nei, opplæringen kunne ha vært bedre», mens 44 % oppgir at de «har fått en del opplæring, men ønsker mer».

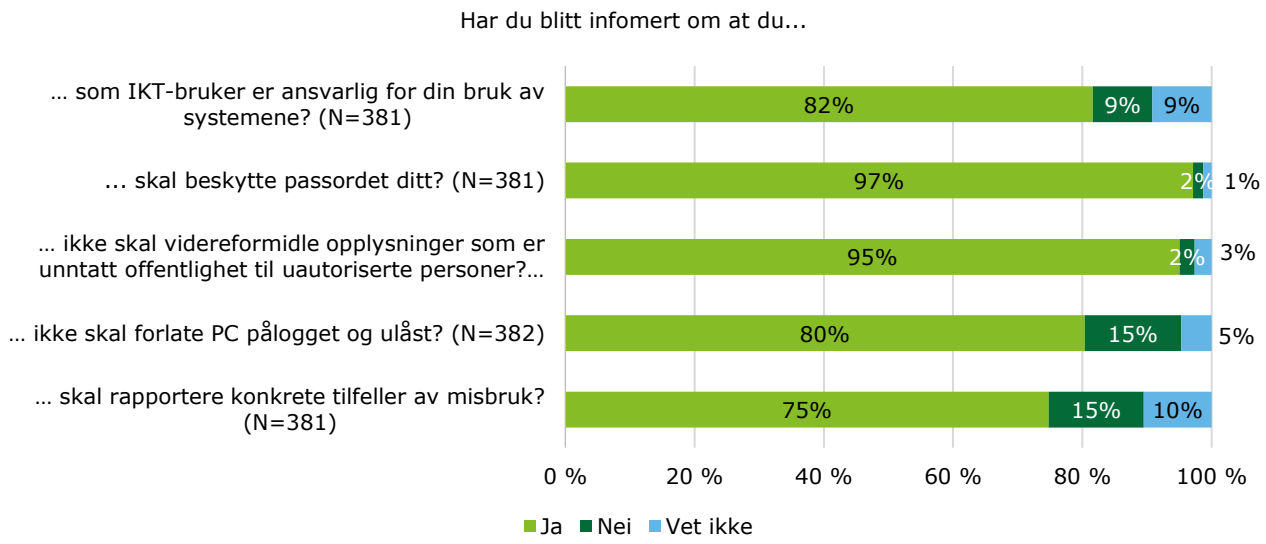
Respondentene som svarte at de ikke har fått opplæring eller ønsker mer/bedre opplæring i håndtering av informasjon og personopplysninger og/eller bruk av IKT-system, fikk et oppfølgingsspørsmål der de kunne kommentere på «hva kan gjøres bedre når det gjelder opplæring knyttet til informasjonssikkerhet og/eller bruk av IKT-systemer».[80] 54 av de 89 respondentene som svarer på oppfølgingsspørsmålet mener at det bør være mer eller bedre opplæring og kursing på området. Noen påpeker at det må settes av tilstrekkelig tid til opplæringen i IKT-systemene og at det som del av dette må være rom for å prøve og feile. Noen av respondentene etterlyser avdelingsvis kurs/møter/opplæring der man kan gå gjennom tema sammen, klargjøre begrep og/eller repetere hvordan man skal håndtere personopplysninger eller bruke IKT-systemet.

En del av respondentene påpeker at det bør utformes enklere og klarere retningslinjer og én respondent legger til at retningslinjene «bør være knyttet opp mot ulike typer enheter som for eksempel skole slik at de oppleves som mer … relevant». Noen av respondentene etterlyser videre at informasjon og retningslinjer på området er lettere tilgjengelig. Én respondent utdyper at det er vanskelig å få oversikt over informasjonssikkerhetstema på *Allmenningen*, da det er lagt inn veldig mye informasjon om temaet (se avsnitt 3.4.1 om tilgang til dokumentene som utgjør styringssystem for personvern og informasjons-sikkerhet på intranett).

Videre fikk respondentene i spørreundersøkelsen spørsmål om hvilken informasjon de eventuelt har mottatt når det gjelder informasjonssikkerhetspraksis. Svarene fremgår i figur 14 under:

[80] N=89

Figur 14: Informasjon om informasjonssikkerhetspraksis



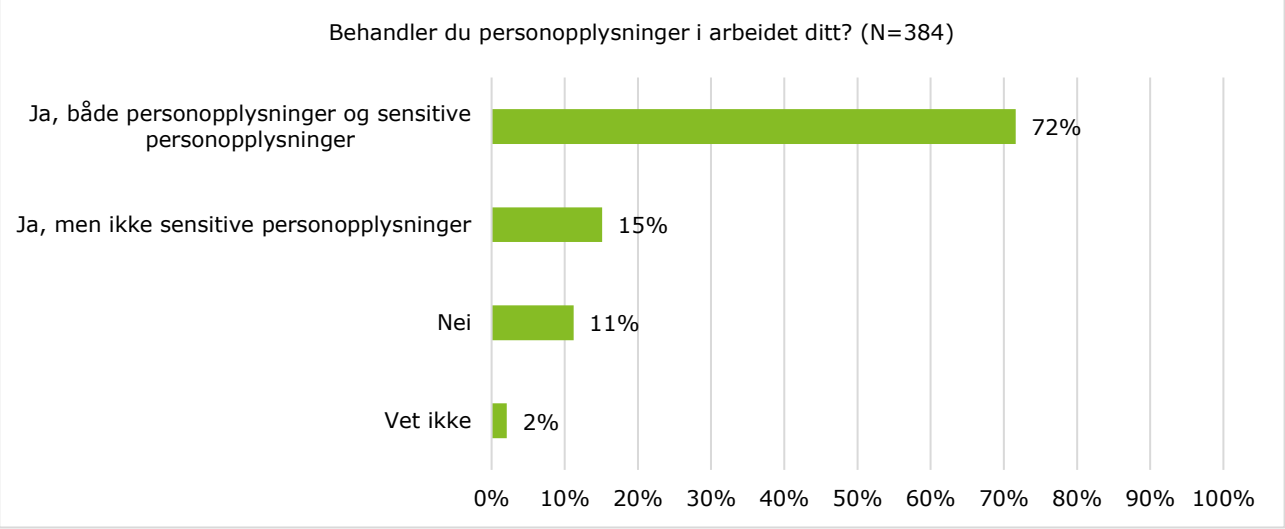
Som gjengitt i figuren over, svarer den store majoriteten av respondentene «ja» på samtlige delspørsmål. 15 % av respondentene svarer at de ikke har blitt informert om at de «ikke skal forlate PC pålogget og ulåst» eller at de skal «rapportere konkrete tilfeller av misbruk». 5 % av respondentene svarer at de ikke har blitt informert eller ikke vet om de har blitt informert om at de «ikke skal videreformidle opplysninger som er unntatt offentlighet til uautoriserte personer». Videre svarer 9 % av respondentene at de ikke har blitt informert om at de er ansvarlig for sin bruk av IKT-systemene, og 9 % vet ikke om de har fått denne informasjonen.

Kompetanse hos de ansatte

Kjennskap til rutiner og retningslinjer

Som vist i figur 15, svarer til sammen 87 % av respondentene i spørreundersøkelsene at de behandler både personopplysninger og sensitive personopplysninger (72 %) eller bare personopplysninger (15 %) i sitt arbeid. På spørsmål om de behandler eller kommer i kontakt med annen fortrolig informasjon i sitt arbeid, svarer 82 % «ja».

Figur 15: Behandling av personopplysninger

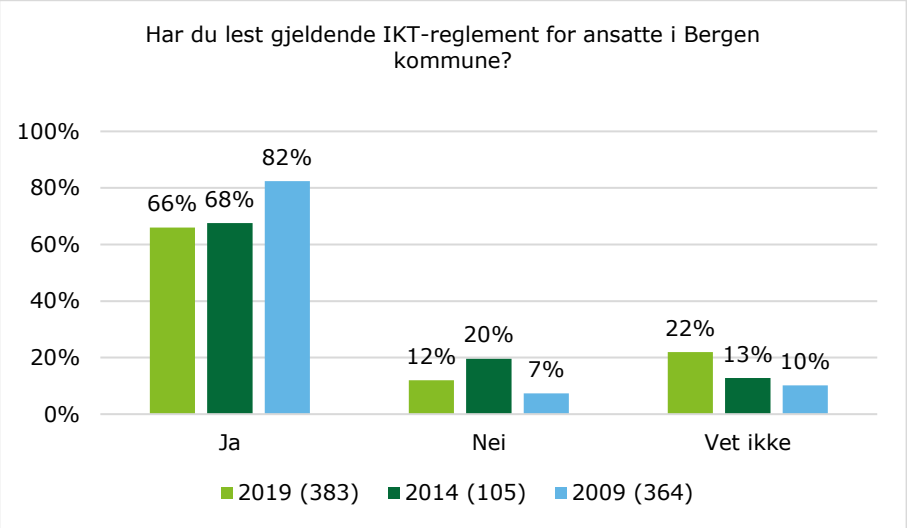


Respondentene i spørreundersøkelsen fikk en rekke spørsmål knyttet til rutiner og retningslinjer og hvorvidt de er kjent med innholdet i disse. De ble blant annet spurt om de er kjent med hvor de finner rutiner og retningslinjer for informasjonssikkerhet/håndtering av personopplysninger, sensitive personopplysninger

og/eller annen fortrolig informasjon som gjelder kommunen/enheten. Totalt svarte 70 % «ja» på dette spørsmålet, mens de resterende 30 % svarte «nei».[81]

Både i årets spørreundersøkelse og dem gjennomført i 2014 og 2009 ble respondentene spurt om de har lest gjeldende IKT-reglement for ansatte i Bergen kommune. Svarene er gjengitt i figur 16:

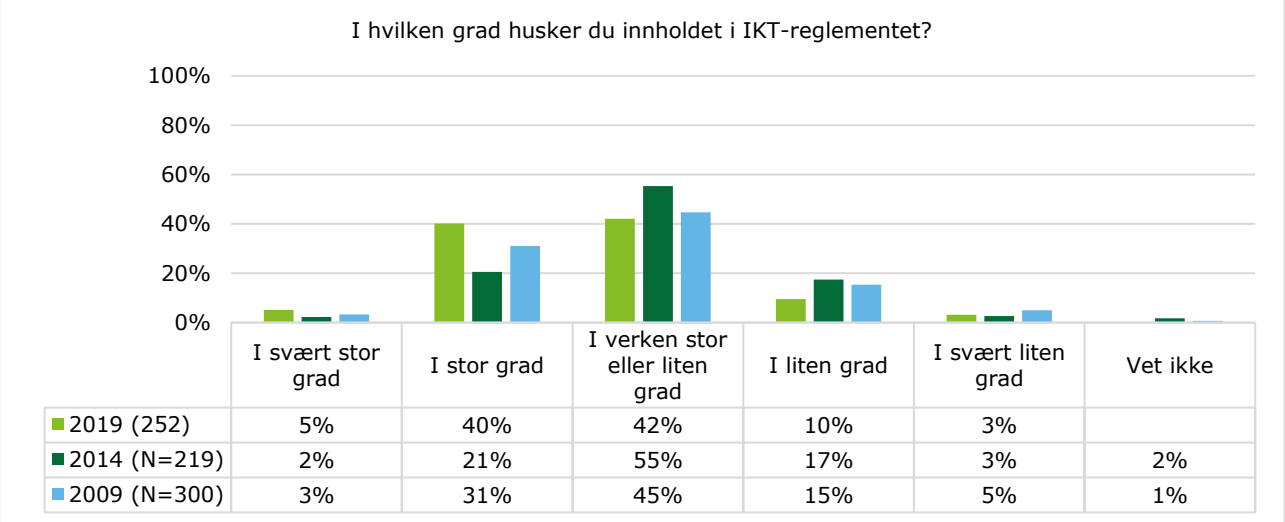
Figur 16: Lest kommunens IKT-reglement



Som vist i figuren, har andelen som svarer «ja» gått ned fra 82 % i 2009, via 68 % i 2014, til 66 % i 2019. Færre svarer «nei» i 2019 enn i 2014, men enda færre svarte «nei» i 2009. Og endelig svarer over en femdel i 2019 at de «ikke vet» om de har lest reglementet, mot henholdsvis 13 % og 10 % i 2014 og 2009.

Respondentene som svarte «ja» på spørsmålet om de har lest IKT-reglementet for ansatte fikk i 2019 videre spørsmål om de husker innholdet i dette reglementet. Svarene fremgår i figur 17:

Figur 17: Husker IKT-reglementet



	I svært stor grad	I stor grad	I verken stor eller liten grad	I liten grad	I svært liten grad	Vet ikke
2019 (252)	5%	40%	42%	10%	3%	
2014 (N=219)	2%	21%	55%	17%	3%	2%
2009 (N=300)	3%	31%	45%	15%	5%	1%

Figuren viser at andelen respondenter som oppgir at de «i stor grad» eller «i svært stor grad» husker innholdet i IKT-reglementet har gått opp i 2019 (45 %) sammenlignet med svarene i de foregående

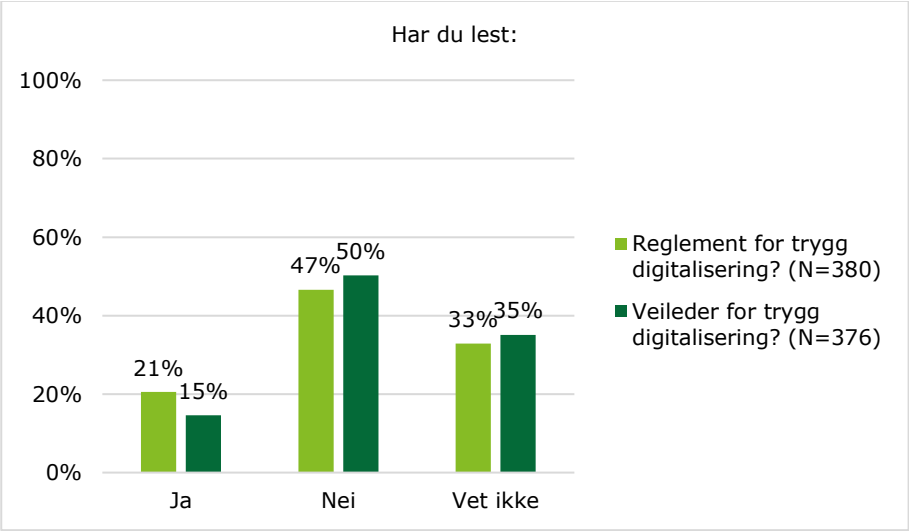
[81] N=378.

undersøkelsene, og tilsvarende at andelen som svarer «i liten grad» eller «i svært liten grad» har gått ned.[82]

Respondentene i 2019-undersøkelsen som svarte at de «i svært stor grad», «i stor grad» eller «i verken stor eller liten grad» husker innholdet i IKT-reglementet, ble bedt om å svare på hvorvidt innholdet i reglementet er forståelig for dem; henholdsvis 64 % og 11 % av respondentene svarte at reglementet «i stor grad» eller «i svært stor grad» er forståelig.[83]

Respondentene fikk også spørsmål knyttet til om de har lest sentrale dokument i styringssystemet for personvern og informasjonssikkerhet. Svarene fremgår i figur 18 under:

Figur 18: Kjennskap til sentrale dokument (alle)



De som svarte «ja» på spørsmålet om de har lest reglement- og veileder for trygg digitalisering fikk oppfølgingsspørsmål på om de husker innholdet i de dokumentene.[84] 11 % av respondentene svarer at de «i liten grad» husker innholdet i *Reglement for trygg digitalisering*, mens 34 % svarer at de «i verken stor eller liten grad» husker innholdet; henholdsvis 47 % og 8 % svarer «i stor grad» og «i svært stor grad».

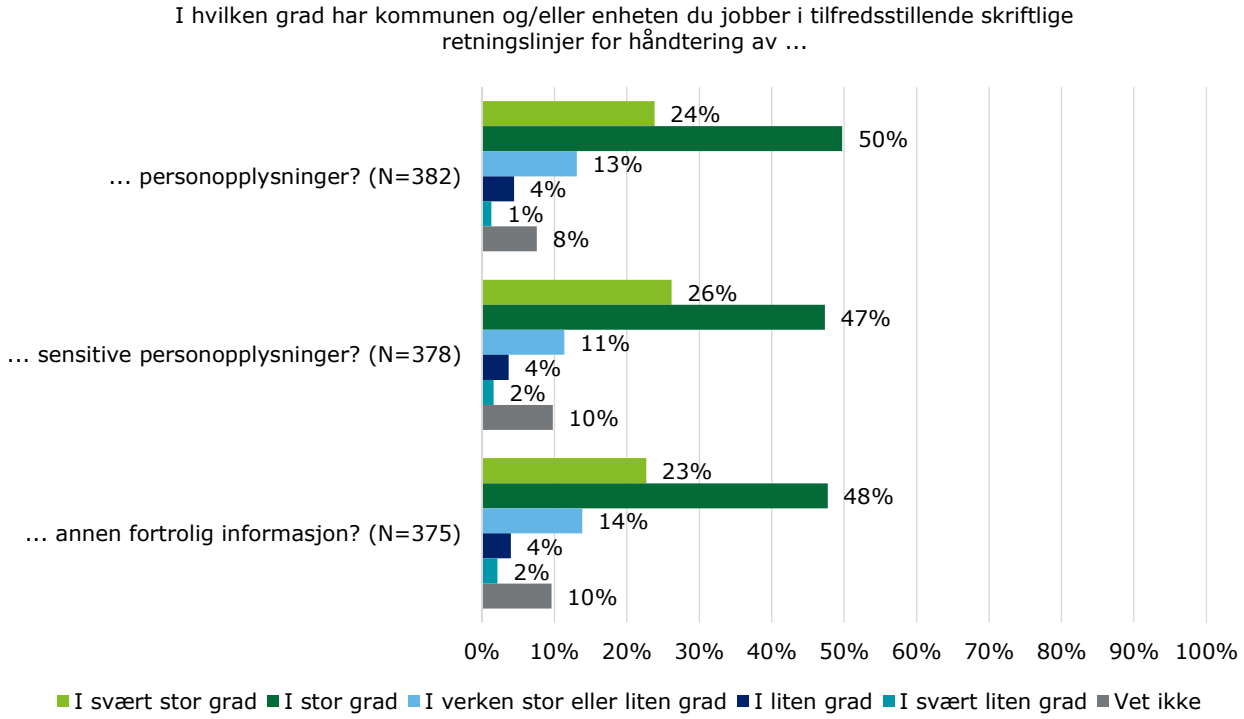
Videre svarer 6 % av respondentene som har lest *Veileder for trygg digitalisering* at de «i liten grad» husker innholdet i denne, 2 % oppgir at de «i svært liten grad» husker innholdet, mens 38 % svarer at de «verken i stor eller liten grad» husker innholdet; henholdsvis 48 % og 6 % svarer «i stor grad» og «i svært stor grad».

De som svarer at de «i svært stor grad», «i stor grad» eller «i verken stor eller liten grad» husker innholdet i veilederen og reglementet fikk et oppfølgingsspørsmål om hvorvidt innholdet var forståelig. De fleste svarer at innholdet i veilederen og reglementet var forståelig for dem.

Deltakerne i spørreundersøkelsen fikk spørsmål om de opplever at kommunen eller enheten de jobber i har tilstrekkelig skriftlige retningslinjer for håndtering av personopplysninger, sensitive personopplysninger og annen fortrolig informasjon. Svarene er fremstilt i figur 19:

[82] I 2009 og 2004 var «vet ikke» et svaralternativ, mens dette svaralternativet ikke var med i spørreundersøkelsen i 2019. Undersøkelsene i 2009 og 2014 hadde også med svaralternativet «i noen grad», som revisjonen i 2019-undersøkelsen erstattet med «i verken stor eller liten grad».
[83] N=213. 24,4 % svarte «i verken stor eller liten grad», 0,9 % (eller to respondenter) svarte «i liten grad», og ingen svarte «i svært liten grad».
[84] «I hvilken grad husker du innholdet i *reglement for trygg digitalisering?*» (N=79), «I hvilken grad er innholdet i *reglement for trygg digitalisering* forståelig for deg?» (N=69), «I hvilken grad husker du innholdet i *veileder for trygg digitalisering*?» (N=52), «I hvilken grad er innholdet i *veileder for trygg digitalisering* forståelig for deg?» (N=46).

Figur 19: Tilfredsstillende skriftlige retningslinjer for informasjonssikkerhet



Av figuren over fremgår det at mellom 8 % og 10 % av respondentene oppgir at de ikke vet om kommunen/ enheten har tilfredsstillende skriftlige retningslinjer på områdene det blir stilt spørsmål om. 4 % av respondentene oppgir at det «i liten grad» foreligger tilfredsstillende skriftlige rutiner for dette, mens om lag halvparten svarer «i stor grad», og nesten en fjerdedel svarer «i svært stor grad».

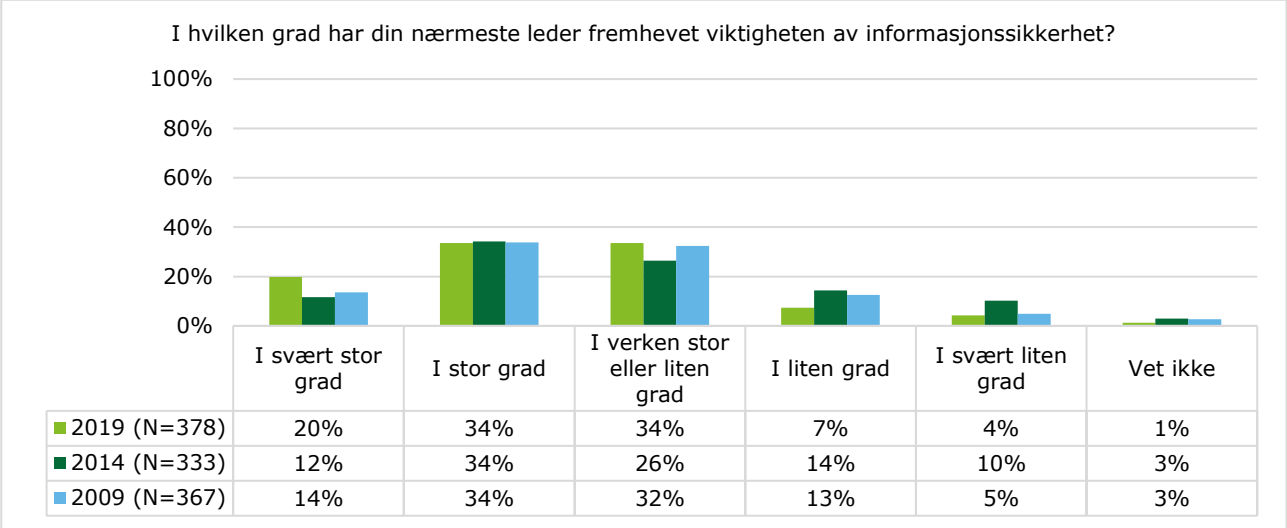
På spørsmål om de kjenner til rutinene for å melde avvik knyttet til informasjonssikkerhet, svarte 32,5 % av de 380 respondentene «nei», 46,5 % «delvis» og de resterende 21 % svarer «ja».[85]

Informasjon om informasjonssikkerhet

Deltakerne i spørreundersøkelsene i 2009, 2014 og 2019 fikk spørsmål om i hvilken grad deres nærmeste leder har fremhevet viktigheten av informasjonssikkerhet. Svarene er gjengitt i figuren under, og disse indikerer en svak tendens med økt fokus på viktigheten av informasjonssikkerhet i kommunen.

[85] På samme spørsmål i 2009 og 2014 svarte henholdsvis 83 % og 62 % av respondentene at de ikke kjente til disse rutinene. Merk at spørreundersøkelsen i 2019 hadde svaralternativet «delvis», noe som ikke var inkludert i undersøkelsene fra 2009 og 2014, og som sannsynligvis påvirker prosentfordelingen på ja/nei.

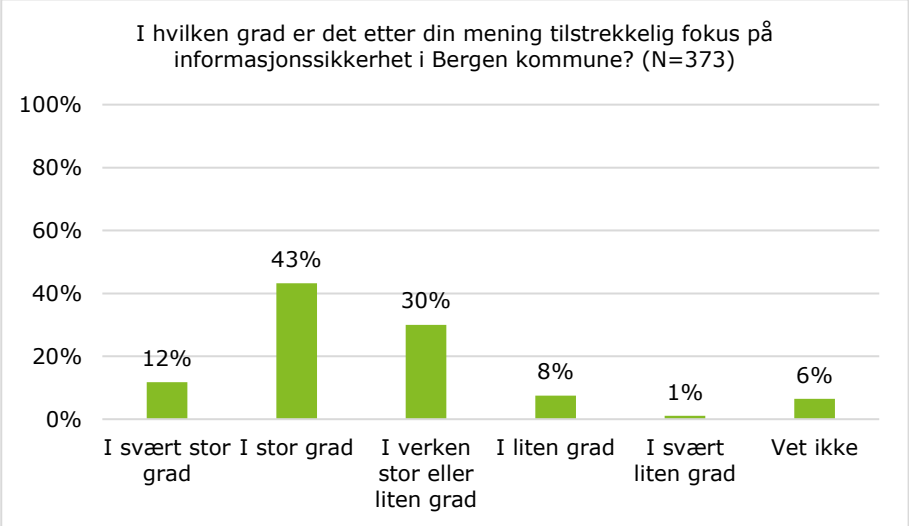
Figur 20: Viktigheten av informasjonssikkerhet



	I svært stor grad	I stor grad	I verken stor eller liten grad	I liten grad	I svært liten grad	Vet ikke
2019 (N=378)	20%	34%	34%	7%	4%	1%
2014 (N=333)	12%	34%	26%	14%	10%	3%
2009 (N=367)	14%	34%	32%	13%	5%	3%

Respondentene i spørreundersøkelsen fikk i tillegg et spørsmål om hvorvidt de mener at det er tilstrekkelig fokus på informasjonssikkerhet i kommunen. Som fremstilt i figur 21 under svarer de aller fleste enten «i svært stor grad» (12 %), «i stor grad» (43 %) eller «i verken stor eller liten grad» (30 %).

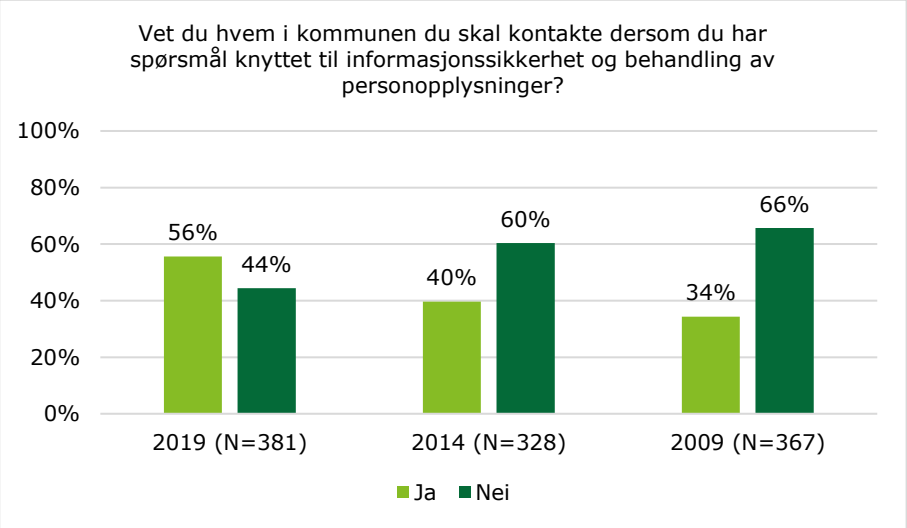
Figur 21: Fokus på informasjonssikkerhet



I spørreundersøkelsene i 2009, 2014 og 2019 ble det stilt spørsmål om respondentene vet hvem i kommunen man skal kontakte dersom man har spørsmål knyttet til informasjonssikkerhet og behandling av personopplysninger.[86] Som fremstilt i figur 22 svarer flere «ja» enn «nei» i 2019, mens det både i 2014 og 2009 var motsatt.

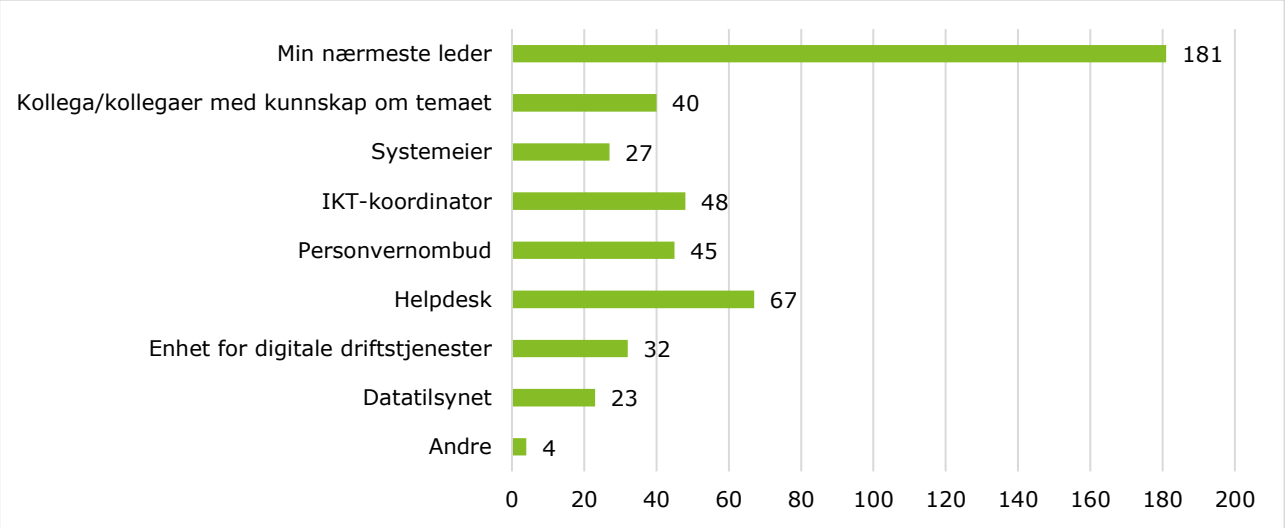
[86] I 2019-undersøkelsen var spørsmålet «vet du hvem i kommunen du skal kontakte dersom du har spørsmål knyttet til informasjonssikkerhet, behandling av personopplysninger og/eller behandling av fortrolig informasjon?»

Figur 22: Kontakt ved spørsmål om informasjonssikkerhet og personvern



I 2019-undersøkelsen fikk respondentene som svarte «ja» på spørsmålet gjengitt i figur 22 videre et oppfølgingsspørsmål om *hvem* de skal kontakter dersom de har spørsmål knyttet til informasjonssikkerhet. Svarene fremgår i figuren under:

Figur 23: Hvem skal du kontakte dersom du har spørsmål knyttet til informasjonssikkerhet? (N=211)[87]



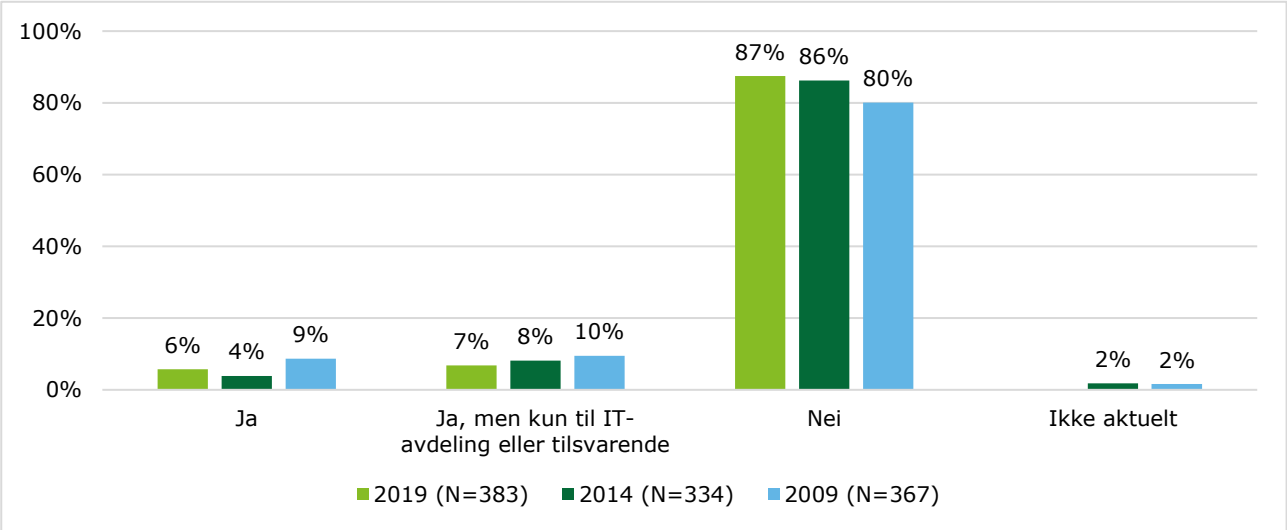
De fire som krysset av for at de ville ha kontaktet «andre» enn de oppgitte alternativene som er gjengitt i figur 23, spesifiserte i et åpent tekstfelt at de enten ville kontaktet seksjon for internkontroll, kommunens mediekontakt, kommuneadvokaten eller media med spørsmål knyttet til informasjonssikkerhet.

Praksis

Deltakerne i undersøkelsene gjennomført i 2009, 2014 og 2019 fikk spørsmål om de «noen gang har lånt ut brukernavn og passord til andre». Samlet andel respondenter som svarer «nei» på dette spørsmålet har økt fra 80 % i 2009 til 86 % i 2014 og endelig til 87 % i 2019 (se figur 24).

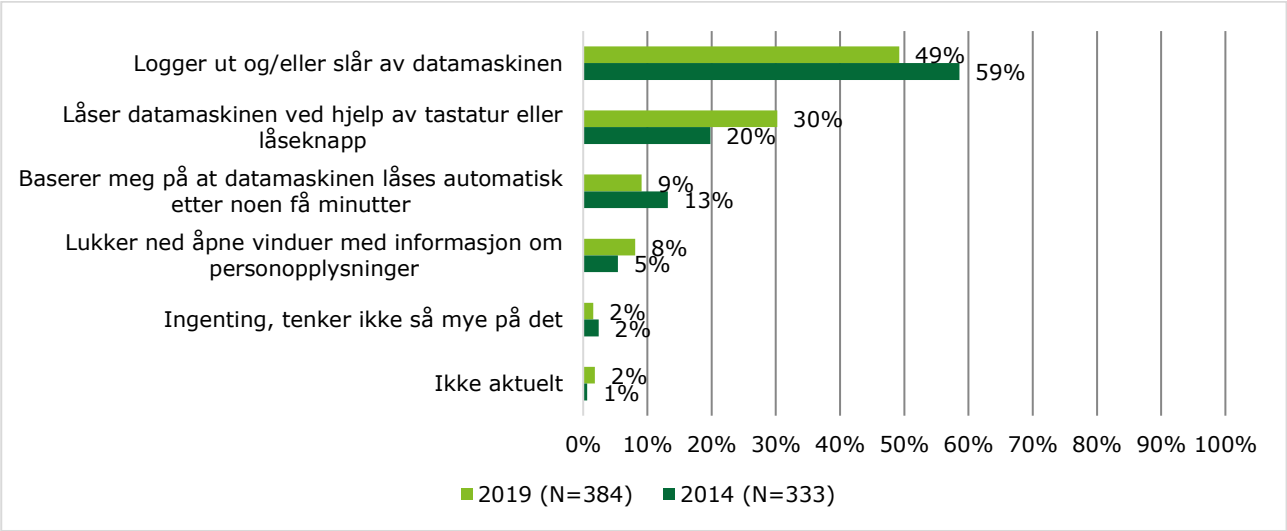
[87] Respondentene kunne krysse av for flere alternativ på dette spørsmålet, og svarene er derfor ikke prosentuert.

Figur 24: Delt passord[88]



Respondentene i 2019- og 2014-undersøkelsene fikk spørsmål om praksis når de forlater PC-en de bruker på arbeidsplassen:

Figur 25: Hva gjør du vanligvis når du i løpet av arbeidsdagen forlater PC-en du bruker?

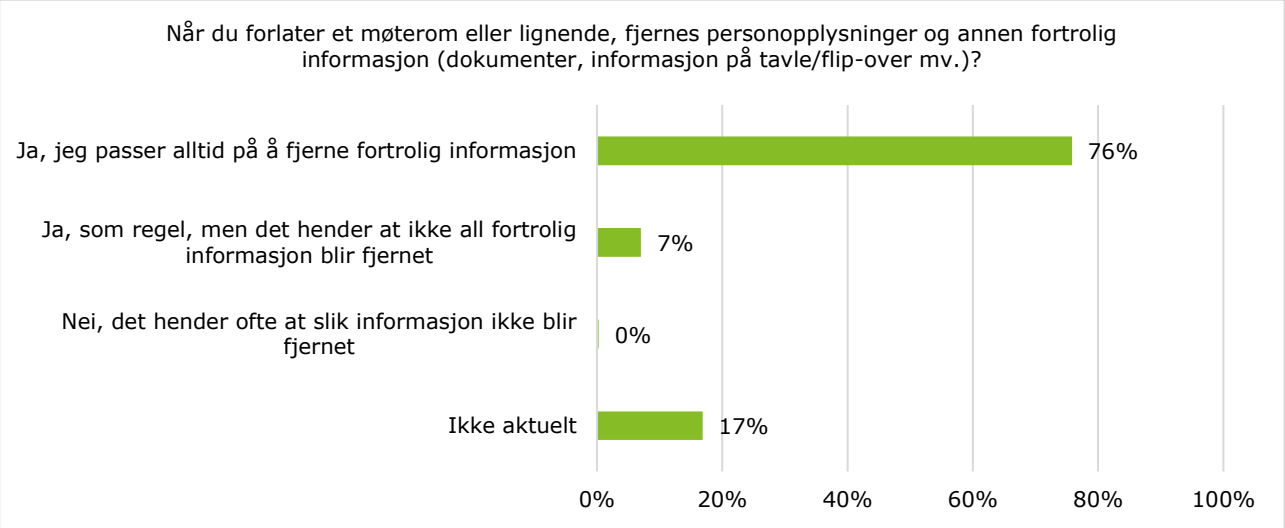


Som vist i figur 25, er det en lavere andel i 2019 enn 2014 som svarer at de «logger ut og/eller slår av datamaskinen» når de forlater arbeidsplassen (49 % mot 59 %), mens det er en økning i andelen som svarer at de «låser datamaskinen ved hjelp av tastatur eller låseknapp» (30 % i 2019, 20 % i 2014). En noe høyere andel svarer videre at de «lukker ned vinduer med informasjon om personopplysninger» i 2019 (8 %) enn i 2014 (5 %).

Respondentene som svarte «ja» på spørsmål om de behandler personopplysninger og/eller sensitive personopplysninger eller om de kommer i kontakt med annen fortrolig informasjon i arbeidet (se figur 15), fikk i spørreundersøkelsen spørsmål om personopplysninger og annen fortrolig informasjon blir fjernet fra møterom når man forlater det. Svarene er fremstilt i figur 26:

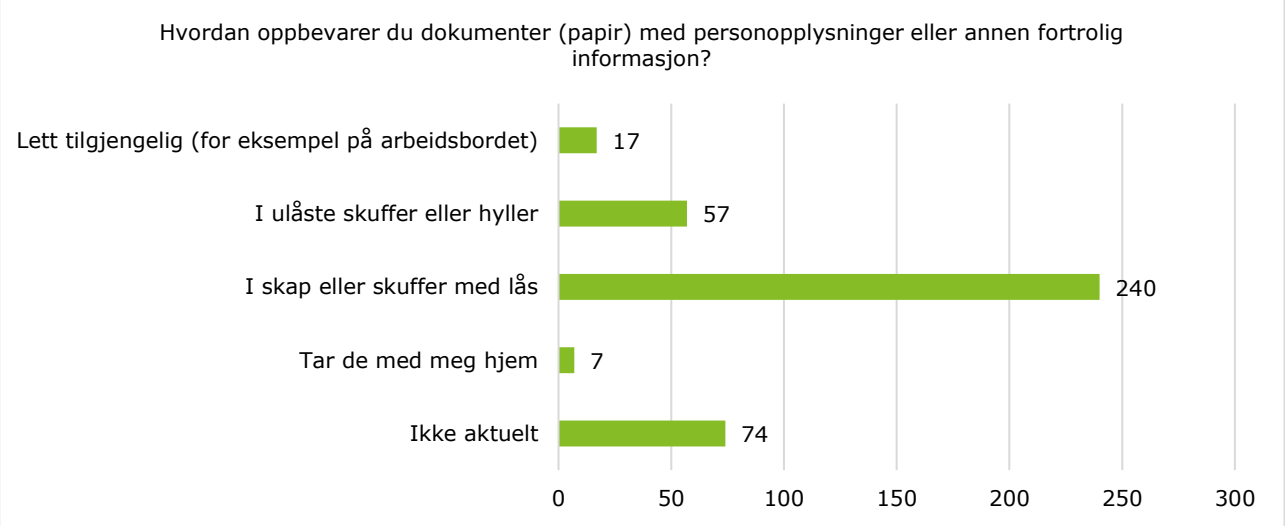
[88] Svarkategorien «ikke aktuelt» var ikke med i undersøkelsen som ble gjennomført i 2019.

Figur 26: Møterompraksis o.l.



De samme respondentene fikk også spørsmål om hvordan de oppbevarer dokumenter (papir) med personopplysninger eller annen fortrolig informasjon. Svarene fremgår i figur 27 under:

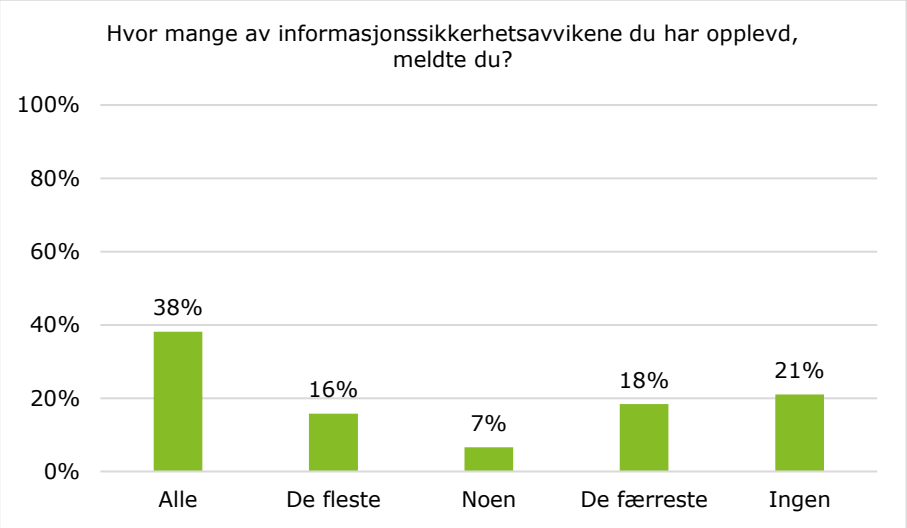
Figur 27: Oppbevaring av dokumenter med personopplysninger eller annen fortrolig informasjon[89]



Respondentene fikk også spørsmål om de har opplevd «ett eller flere informasjonssikkerhetsavvik». Totalt svarte 22 % «vet ikke» på dette spørsmålet, mens 20 % svarer «ja» og 58 % svarer «nei». De 20 % som svarte «ja» fikk oppfølgingsspørsmål knyttet til hvorvidt de har meldt fra om avvikene.[90] Resultatene på dette spørsmålet fremgår i figur 28:

[89] Respondentene kunne krysse av for flere alternativ på dette spørsmålet, og svarene er derfor ikke prosentuert.
[90] N=76.

Figur 28: Meldte avvik (N=76)



Totalt oppgir altså 21 % av de som har opplevd informasjonssikkerhetsavvik at de ikke har meldt noen av dem, mens 18 % svarer at de har meldt «de færreste». 7 % av respondentene oppgir at de har meldt «noen» informasjonssikkerhetsavvik.

Respondentene som svarte «alle», «de fleste», «noen» eller «de færreste» fikk spørsmål om oppfølgingen av innmeldte avvik. Totalt svarer 33 % at de ikke vet om meldingen om informasjonssikkerhetsavvik er fulgt opp.[91] 11 % svarer «nei» på spørsmålet om meldte avvik har blitt fulgt opp, mens 13 % oppgir at avvikene «delvis» har blitt fulgt opp. De resterende 43 % svarte «ja».

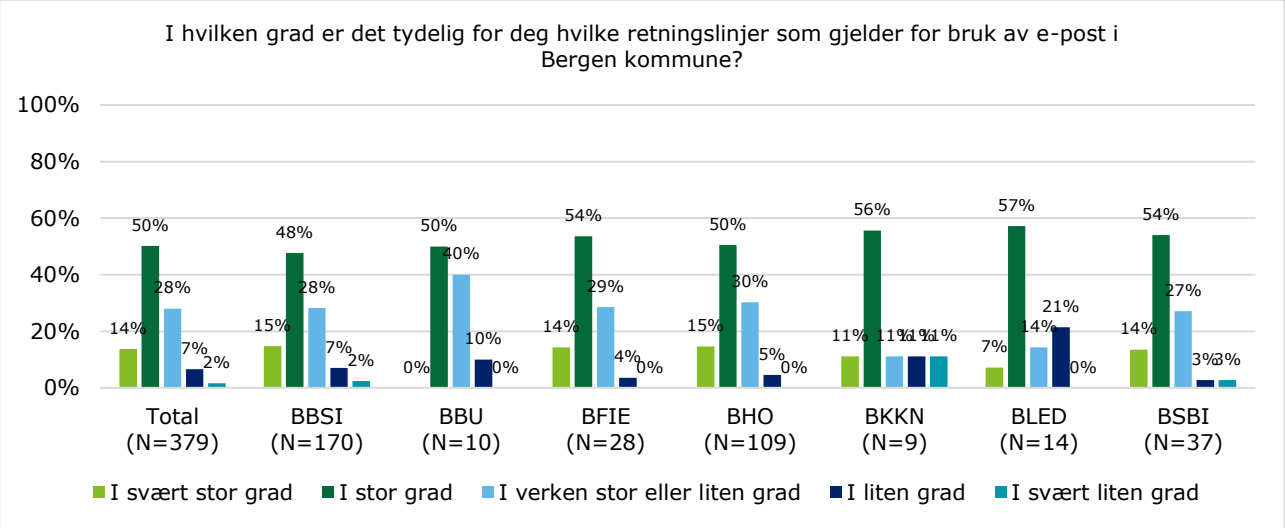
Respondentene fikk mulighet til å komme med tilbakemelding på områder der «Bergen kommune kan forbedre sin behandling av personopplysninger».[92] Noen av respondentene kommer her med tilbakemeldinger på manglende tilgangsstyring til ulike systemer som benyttes i kommunen, en del nevner behov for mer kurs og opplæring på området og en del nevner utfordringer med det nylig innførte saksbehandlingssystemet BK360. Videre er det en del som tar opp bruk av e-post i kommunen og blant annet behov for opplæring/informasjon knyttet til å kryptere innhold i e-poster.

Trygg e-postbruk – kompetanse og etterlevelse

I spørreundersøkelsen fikk deltakerne spørsmål om i hvilken grad de mente det er tydelig hvilke retningslinjer som gjelder for bruk av e-post i Bergen kommune. Svarene fremgår i figuren under, med totalen først og deretter svarene per byrådsavdeling:[93]

[91] N=61
[92] N=51 (17 av respondentene svarer nei/vet ikke/usikker).
[93] Pga. få respondenter er svarene fra bystyrets administrasjon utelatt.

Figur 29: Tydelige retningslinjer for bruk av e-post



Som fremstilt i figuren over svarer nesten 30 % av respondentene at det «i verken stor eller liten grad» er tydelig hvilke retningslinjer som gjelder for bruk av e-post i kommunen, mens 7 % oppgir at dette «i liten grad» er tydelig. Totalt svarer 2 % av respondentene at retningslinjene for bruk av e-post i kommunen «i svært liten grad» er tydelig.

For å teste om og i hvilken grad ansatte i Bergen kommune praktiserer trygg e-postbruk, gjennomførte revisjonen et nettfiskeforsøk (phising) der 13 365 ansatte i Bergen kommune fikk tilsendt en falsk e-post. Testen er utformet for å måle i hvor stor utstrekning ansatte 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 kommunen.[94]

Det er viktig å understreke at formålet med testen var å undersøke om *ansatte* 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 autentiske 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.[95] 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.[96] Det er

[94] 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.
[95] 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.
[96] I forbindelse med verifiseringen av rapporten opplyser kommunen at flere ansatte i etterkant av forsøket har opplyst 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.[97]

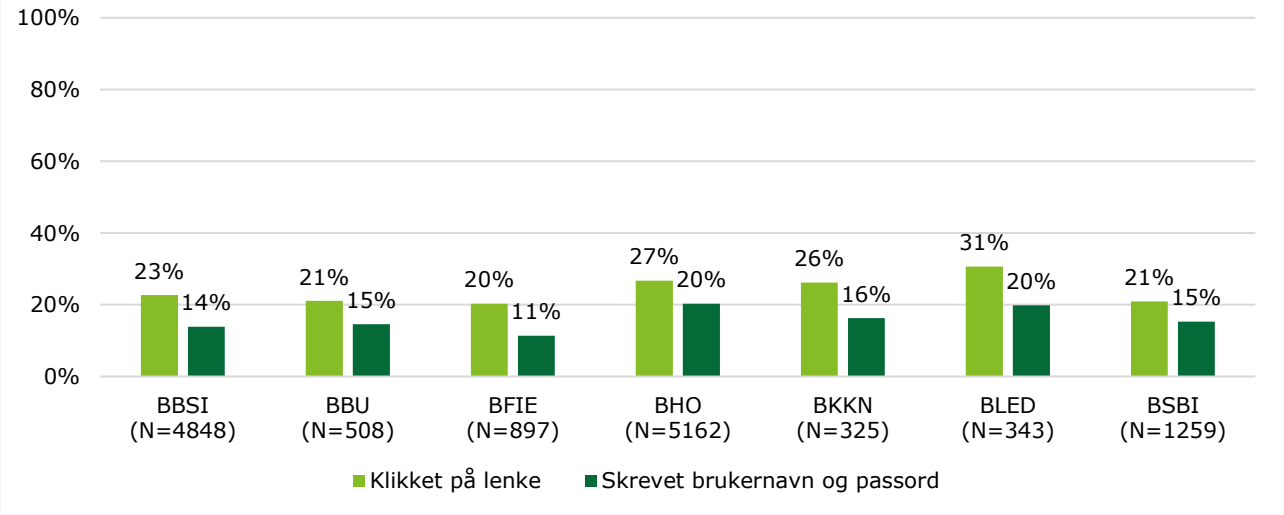
Målgruppen i nettfiskeforsøket mottok 15. mai en e-post fra avsenderen «Dcure Global» med invitasjon til en etikkundersøkelse for Bergen kommune. For å besvare undersøkelsen ble mottakerne bedt om å trykke på en lenke i e-posten.

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 3226 på lenken. Av disse skrev 2213 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. Figur 30 viser resultatene av nettfiskeforsøket fordelt per byrådsavdeling.[98] Som det går frem i denne, varierer andelen som klikket på lenken i e-posten med mellom 20 % og 31 %, mens andelen som skrev inn sitt brukernavn og passord varierte mellom 11 % og 20 %.

Figur 30: Resultater nettfiskeforsøk per byrådsavdeling



5.4 Vurdering

Opplæring

Undersøkelsen viser at kommunen har obligatoriske kurs for både nyansatte og ledere der informasjons-sikkerhet inngår som tema, at det tilbys ulike nettkurs knyttet til informasjonssikkerhet, at det

[97] Kommunen publiserte en nyhetssak om nettfiskeforsøket på *Allmenningen* etter at forsøket var avsluttet.
[98] Resultatene fra bystyrets administrasjon og byombudet er ikke presentert av personvernhensyn. Resultatene fra disse skilte seg ikke nevneverdig fra resten.

gjennomføres informasjonssikkerhetskampanjer, og at veiledningsmateriell innenfor ulike informasjonssikkerhetstema er tilgjengeliggjort for de ansatte. Kommunen stiller videre som vilkår for bruk av IKT-systemene at ansatte har lest og akseptert *Reglement for akseptabel bruk av IKT*. 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 resultatenhetslederne bare delvis oppgir å 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 om lag 60 % av respondentene oppgir å ikke ha fått tilstrekkelig opplæring knyttet til personvern og informasjonssikkerhet, og tre firedeler 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; totalt 18 % 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, 20 % 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 25 % 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 informasjonssikkerhetskompetanse blant de ansatte gjennom opplæringstiltak (f.eks. ISO27001:2013 punkt 7.2).

Dette medfører at det er høyere sannsynlighet for at de ansatte 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 knyttet til informasjonssikkerhetskompetanse og –praksis (se under) tyder videre på at denne risikoen har gjort seg gjeldende.

Kompetanse

Undersøkelsen viser at majoriteten av respondentene behandler personopplysninger, sensitive personopplysninger eller annen fortrolig informasjon i sitt arbeid. Likevel svarer 30 % av respondentene at de ikke vet hvor de finner kommunen sine retningslinjer for hvordan slike opplysninger skal håndteres.

Revisjonen merker seg videre at om lag én av fem respondenter 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 én av fem av respondentene at de har lest *Reglement for trygg digitalisering*, kommunens overordnete reglement for informasjonssikkerhet, mens halvparten svarer at de *ikke* har lest *Veileder for trygg digitalisering*. Kun om lag én av fem svarer «ja» på spørsmålet om de kjenner rutinene for å melde avvik knyttet til informasjonssikkerhet.

Sett i sammenheng med funnene i for eksempel kapittel 3, mener revisjonen at kommunen oppfyller første del av anbefaling nr. 3 fra 2015 om å «sørge for at retningslinjer og rutiner på informasjonssikkerhet er oppdatert», men altså ikke andre del, om å «sikre at alle ansatte kjenner til hvor man finner rutinene».

Basert på funnene i undersøkelsen, er det revisjonen sin vurdering at ikke alle ansatte 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.

Praksis

Med hensyn til informasjonssikkerhetspraksis, viser undersøkelsen blant annet at nesten en femdel av respondentene ikke følger en praksis for avlogging eller låsing av datamaskinen i samsvar med prinsipper om god informasjonssikkerhet. Videre viser undersøkelsen at 13 % av respondentene enten har delt passordet sitt med IT-avdelingen eller andre. Revisjonen vil i den forbindelse understreke at det å dele passord med andre ikke er i samsvar med grunnleggende prinsipp for informasjonssikkerhet, heller ikke dersom det er IT-avdelingen man deler passordet med.

Det fremgår videre i spørreundersøkelsen at av respondentene som har opplevd informasjonssikkerhets-avvik, meldte totalt 39 % «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 33 % 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.

Også resultatene fra nettfiskeforsøket viser at ansatte i Bergen kommune har en svak informasjons-sikkerhetspraksis; nesten én av fire (litt over 24 %) valgte å trykke på lenken i e-posten, og 16,5 % oppgav sitt brukernavn og passord.

Basert på funnene i undersøkelsen, er det revisjonen sin vurdering at de ansatte i Bergen kommune ikke i tilstrekkelig grad etterlever retningslinjer og rutiner for informasjonssikkerhet, og videre at informasjons-sikkerhetspraksisen blant de ansatte bryter med flere grunnleggende informasjonssikkerhetsprinsipp.

6. Konklusjon og anbefalinger

I denne forvaltningsrevisjonen har Deloitte undersøkt om Bergen kommunen har et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket, og i hvilken grad dette etterleves. Forvaltningsrevisjonen har vært en oppfølging av tilsvarende forvaltningsrevisjoner gjennomført i 2009 og 2014.

Tilfredsstillende informasjonssikkerhet

Bergen kommune har et oppdatert styringssystem for personvern og informasjonssikkerhet. Det er ikke avdekket funn i undersøkelsen som tyder på at dette ikke er i samsvar med kravene i gjeldende regelverk. Kommunen har gjennom styringssystemet etablert prosedyrer, retningslinjer og systemer som er egnet til å utbedre flere av svakhetene påpekt i revisjonen fra 2015. Samtidig registrerer revisjonen at praksis på flere av de samme områdene fortsatt har forbedringspotensial.

Kommunen har prosedyre for melding av avvik som er i samsvar med regelverket, og system som legger til rette for melding av avvik. Tilsendt avviksstatistikk og svar i spørreundersøkelsen tyder imidlertid på at kommunens avvikspraksis ikke fullt ut samsvarer med relevante anbefalinger eller generelle prinsipper for god internkontroll. Revisjonen mener at kommunen bare delvis har fulgt opp anbefaling nr. 1c fra 2015.

Kommunen har også etablert verktøy og retningslinjer for gjennomføring av risikovurderinger, og gjennomfører slike. Selv om kommunen har gjort fremskritt på dette området siden 2015, er flere av risikovurderingene mangelfulle, og flere systemer mangler risikovurderinger. Revisjonen mener derfor kommunen bare delvis har fulgt opp anbefaling nr. 1a fra 2015.

I styringssystemet stilles det krav om gjennomføring av sikkerhetsrevisjoner. Det har blitt gjennomført slike, og etter planen skal det gjennomføres flere. Omfanget av sikkerhetsrevisjoner er imidlertid lavt, og på grunn av manglende og mangelfulle risikovurderinger, har ikke kommunen grunnlag for å velge ut de områdene og systemene for sikkerhetsrevisjon der risikoen for brudd på informasjonssikkerheten er størst. Revisjonen mener kommunen bare delvis har fulgt opp anbefaling nr. 1b fra 2015.

Styringssystemet stiller krav til og inneholder prosedyrer for gjennomføring av ledelsens gjennomgang. Gjennom reetableringen av informasjonssikkerhetsforum høsten 2018 er de organisatoriske forutsetningene for å kunne gjennomføre ledelsens gjennomgang på plass, og ledelsens gjennomgang ble også gjennomført for 2018. Revisjonen mener kommunen langt på vei har fulgt opp anbefaling nr. 1d fra 2015.

Kommunen har en informasjonssikkerhetsstrategi, men denne er ikke styrende for informasjonssikkerhetsarbeidet i kommunen. Kommunen har plan om å rullere eller ev. utarbeide ny informasjonssikkerhetsstrategi, og derigjennom følge opp anbefaling nr. 4 fra 2015.

Tilgangsstyring

Bergen kommune har system og rutiner for tilgangsstyring. Disse vurderes å bare i noen grad være egnet til å sikre at ansatte i kommunen får tilgangene de trenger, og for å sikre at ansatte som slutter i kommunen mister tilgangene sine. Kommunens rutine og praksis knyttet til tilgangsstyring ved skifte av arbeidssted i kommunen vurderes som sårbar, både på grunn av organisatoriske og tekniske forhold.

De gjennomførte sikkerhetstestene avdekket ingen kritiske sårbarheter i kommunens eksterne eller interne nett. Det ble imidlertid identifisert sårbarheter med både høy, moderat og lav risiko. Disse medfører risiko for brudd på informasjonssikkerheten i kommunens informasjonssystemer.

Etterlevelse av utvalgte lovkrav

Bergen kommune har etablert system og praksis for melding om behandling av personopplysninger og utarbeidelse av protokoller med oversikt over slike behandlinger, og har også utarbeidet slike protokoller. Disse er imidlertid i ulik grad av ferdigstillelse, og kommunen har ikke fullstendig oversikt over alle systemene der det muligens behandles personopplysninger. Manglende fullstendighet i oversikt og protokoller gjør at kommunen ikke fullt ut oppfyller relevante krav i personvernforordningen.

Kommunen har retningslinjer, rutiner og verktøy for vurdering av personvernkonsekvenser, og det kommer ikke frem indikasjoner på at disse bryter med krav i regelverket. Kommunen har gjennomført noen vurderinger av personvernkonsekvenser. Manglende risikovurderinger kombinert med mangelfull oversikt over hvilke personopplysninger som behandles betyr imidlertid at kommunen ikke har full oversikt over hvilke personopplysninger som behandles med høy risiko, og derfor heller ikke har tilstrekkelig kunnskapsgrunnlag for å gjennomføre vurdering av personvernkonsekvenser ved behandling av personopplysninger med høy risiko, jf. krav i personvernforordningen.

Kommunen har et personvernombud. Det kommer ikke frem indikasjoner på at mandatet til stillingen ikke oppfyller krav i personvernforordningen. Bergen kommune har også en personvernerklæring, og heller ikke her er det indikasjoner på at denne ikke er i samsvar med krav i personvernforordningen.

Helhetlige føringer

Styringssystemet for personvern og informasjonssikkerhet med tilhørende dokumenter gir felles føringer for informasjonssikkerhet, og det er slik lagt til rette for en oppdatert og helhetlig tilnærming til informasjonssikkerhet i kommunen. Kommunen oppfyller slik første del av anbefaling nr. 3 fra 2015 om å «sørge for at retningslinjer og rutiner på informasjonssikkerhet er oppdatert».

Respondentene i spørreundersøkelsen er i relativt liten grad kjent med hvor de finner relevante rutiner og retningslinjer, og i enda mindre grad har de lest og gjort seg kjent med obligatoriske og sentrale styrende dokumenter. Revisjonen mener derfor det bør iverksettes tiltak for å sikre at styringssystemet faktisk blir etterlevd.

Oppgaver og ansvar

Ansvar og oppgaver knyttet til informasjonssikkerhet fremgår i kommunens styringssystem. Konsernansvaret for informasjonssikkerhet er tydelig lagt til BFIE, og det foreligger fullmakter og avtaler som plasserer ansvar og oppgaver nedover i byrådsavdelingen. Det fremgår videre hvilket ansvar som påhviler ulike roller, samt hvilke oppgaver disse skal utføre for å sikre god informasjonssikkerhet; blant annet er både ansvaret og de respektive oppgavene til resultatenhetsledere, systemeiere og ansatte skriftliggjort.

Funn i undersøkelsen tyder imidlertid på at verken systemeierne eller resultatenhetslederne i tilstrekkelig grad er sitt informasjonssikkerhetsansvar bevisst. Sett i sammenheng med funn knyttet til respondentenes kjennskap til og etterlevelse av kommunens regelverk, rutiner, veiledere, prosedyrer mm. for informasjonssikkerhet (se under), mener revisjonen at Bergen kommune ikke i tilstrekkelig grad har tydeliggjort ansvar og oppgaver knyttet til informasjonssikkerhet.

Funn i undersøkelsen tyder òg på at kommunen ikke i tilstrekkelig grad har sørget for at «systemeiere har tilstrekkelig opplæring og støtteverktøyer for å kunne gjennomføre sine oppgaver», og slik ikke fulgt opp anbefaling nr. 2 fra 2015.

Revisjonen registrerer at blant annet kommunens størrelsen og den parlamentariske styringsmodellen i kommunen fremholdes som medvirkende årsaker til at det kan være utfordrende for BFIE å fullt ut sikre at de enkelte byrådsavdelinger ivaretar sitt ansvar for informasjonssikkerhet. Revisjonen vil understreke viktigheten av at den enkelte byrådsavdeling i kommunen følger opp sitt ansvar for å etterleve kommunens styringssystem for personvern og informasjonssikkerhet, for eksempel ved å sikre at deres representant i informasjonssikkerhetsforum har tilstrekkelig myndighet.

Opplæring, kompetanse og praksis

Bergen kommune har lagt til rette for at ansatte kan tilegne seg kunnskap og kompetanse knyttet til informasjonssikkerhet og personvern gjennom blant annet obligatoriske kurs og veiledningsmateriell. Svarene i spørreundersøkelsen indikerer imidlertid at en relativt stor del av resultatenhetslederne bare delvis oppgir å ha besørget nødvendig opplæring for sine ansatte knyttet til informasjonssikkerhet. Dette reflekteres i svar 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 det er relativt kort tid siden styringssystemet ble etablert, men vil likevel påpeke at Bergen kommune ikke oppfyller krav og anbefalinger om å sikre tilstrekkelig informasjonssikkerhetskompetanse blant de ansatte gjennom opplæringstiltak. Dette understøttes av funn i

undersøkelsen som viser at ikke alle ansatte i Bergen kommune har tilstrekkelig kjennskap til retningslinjer og rutiner for informasjonssikkerhet, at ansatte i Bergen kommune ikke i tilstrekkelig grad etterlever retningslinjer og rutiner for informasjonssikkerhet, samt at informasjonssikkerhetspraksisen blant ansatte bryter med flere grunnleggende informasjonssikkerhetsprinsipp. Revisjonen mener derfor kommunen ikke har fulgt opp andre del av anbefaling nr. 3 fra 2015 om å «sikre at alle ansatte kjenner til hvor man finner rutinene».

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

1) at sentrale aktiviteter i styringssystemet praktiseres som forutsatt, inkludert at det gjennomføres:
    a) risikovurderinger
    b) sikkerhetsrevisjoner
    c) ledelsens gjennomgang
2) at protokoller over behandlinger av personopplysninger er fullstendige og ajourførte
3) at oversikt over databehandleravtaler er fullstendig og ajourført
4) at styringssystemet etterleves i hele kommunen
5) at både systemeiere og resultatenhetsledere 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
7) at det ved utarbeidelse av ny strategi for informasjonssikkerhet blir fastsatt krav til oppfølging av og rapportering på gjennomføring av tiltak, samt eventuell rullering av planer og tiltak
8) at identifiserte organisatoriske risikoer knyttet til tilgangsstyring reduseres
9) at identifiserte tekniske risikoer i kommunens informasjonssystemer reduseres

Vedlegg 1: Høringsuttalelse

BERGEN KOMMUNE

BYRÅDSAVDELING FOR FINANS, INNOVASJON OG EIENDOM
Seksjon for administrasjon

DELOITTE AS AVD BERGEN
Postboks 6013
5892 BERGEN

Vår referanse: 2019/70398-2
Saksbehandler: Ingvild Kvilekval
Dato: 9. september 2019
Deres ref.:

Unntatt offentlighet: Offl § 5

Høringsuttalelse - Rapport etter forvaltningsrevisjon av informasjonssikkerhet i Bergen kommune

Byrådsavdeling for finans, innovasjon og eiendom har mottatt høringsutkast til rapport fra forvaltningsrevisjon av informasjonssikkerhet. Byrådsavdelingen har gått gjennom høringsutkastet, og finner at dette fremstår både grundig og balansert. Vi har opplevd prosessen knyttet til revisjonen som god i de fleste faser av arbeidet. Selv om vi ikke på alle punkter fullt ut deler revisors oppfatninger, ser vi at rapporten er nyansert og at vi kan ha stor nytte av den i det pågående arbeidet med å videreutvikle kommunens systemer og praksis på informasjonssikkerhetsområdet. Som rapporten viser er der fortsatt forbedringspotensiale på flere områder.

Det er kun på ett område vi i denne høringsuttalelsen ser behov for å kommentere funn og anbefalinger særskilt, og det er revisjonens nettfiskeforsøk (Phishing Awareness Test). Som vi har tatt opp med revisor underveis i revisjonsprosjektet, og også gitt tilbakemelding om i verifikasjonen av rapporten, mener vi at 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 kommunen har rundt håndtering av hendelser. Bergen kommune måtte registrere avsenderadressen i sine spam-filter for at mailen skulle nå de ansatte. Da Helpdesk ble kontaktet av ansatte som hadde mottatt eposten, ville det normalt ha blitt sperret for lenken i eposten. Videre ville IKT-kontakter blitt varslet via SMS om hendelsen, og det ville blitt lagt ut informasjon på Bergen kommunes intranett. Siden revisor ba om at kommunen skulle avstå fra å gi informasjon i tilknytning til testen, også ved direkte henvendelser om saken fra ledere og ansatte, ble både kommunens sikkerhetsfunksjon og kommunens informasjonsfunksjon satt ut av spill. I vurderingen av undersøkelsens funn bør dette vektlegges.

Revisor fremholder i sin rapport at hensikten med nettfisketesten var å teste om og i hvilken grad ansatte i kommunen praktiserer trygg epostbruk. Det vil neppe være mulig for Bergen kommune å sikre at alle ansatte til enhver tid har optimal kunnskap og beredskap for trygg epostbruk, i alle fall ville det medføre en stor omkostning med tanke på at det i organisasjonen hele tiden er turnover, at mange arbeider i turnus, at en stor andel av de ansatte arbeider deltid osv. Som ellers i den kommunale driften må det legges til grunn kost-nytte vurderinger ved valg av hvilke tiltak som skal settes i verk, og innsatsen bør rettes mot tiltak som forventes å gi god måloppnåelse.

Som resultatene av revisors nettfisketest viser, blir det viktig for kommunen å arbeide for å styrke informasjonssikkerhetspraksisen blant de ansatte, innenfor de rammer som er mulig å gjennomføre gitt organisasjonens størrelse og sammensetning. Samtidig vil det, ut fra byrådsavdelingens faglige vurderinger, være nødvendig å satse tungt på effektive tekniske

Postadresse:
Postboks 7700, 5020 BERGEN
Kontoradresse:
Rådhusgaten 10

Telefon: 55566422
E-post:
Internett: www.bergen.kommune.no

virkemidler for å sikre kommunen mot nettfisking og andre inntrengingsforsøk i kommunens systemer. Vi mener at kommunens beredskap og risikoreduserende tiltak på systemnivå og individnivå må ses i sammenheng. Det vil være effektene av kommunens samlete tiltak som vil være det vesentlige ved en autentisk hendelse.

I arbeidet med kontinuerlig forbedring og videreutvikling av Bergen kommunes informasjonssikkerhet vil vi nøye gå gjennom revisors funn og anbefalinger. Informasjonssikkerhetsforum vil være en viktig arena for diskusjoner, avklaringer og prioriteringer knyttet til oppfølgingen av rapporten.

Med hilsen

Tor Corneliussen - kommunaldirektør
Kjetil Århus – direktør for digitalisering og innovasjon

Dokumentet er godkjent elektronisk.

Vedlegg 2: 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.[99] Denne trådde i kraft 20. juli 2018, og gjennomfører EU sin personvernforordning – kjent som GDPR[100] – 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.[101] 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 egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med

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

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 frem 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 frem av artikkel 39. Her går det frem 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 frem 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:

> 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.»

I Datatilsynet sin veileder *Internkontroll og informasjonssikkerhet*[102] omhandler blant annet oppfølging og opplæring. Her går det frem 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 frem 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
    a) risikovurderinger
    b) sikkerhetsrevisjoner
    c) avvikshåndtering
    d) ledelsens gjennomgang
2. Sørge for at systemeiere har tilstrekkelig opplæring og støtteverktøyer for å kunne gjennomføre sine oppgaver.
3. 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.

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

Vedlegg 3: 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

Veiledere og standarder

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

Dokumenter fra kommunen

- Strategi for informasjonssikkerhet. Bergen kommune.
- Overordnet rutine for håndtering av avvik som gjelder personvern og informasjonssikkerhet.
- Avviksoversikt 08.08.2018 – 14.03.2019
- Prosedyre for ledelsens gjennomgang
- Avslutning av arbeidsforhold. Sjekkliste for leder
- Protokoll over behandlingsaktiviteter etter artikkel 30 i personvernforordningen – alle byrådsavdelingene
- Sikkerhetsrevisjonsrapporter 2015, 2016 og 2019
- Inntrengningstest 2016, 2017 og 2018
- Oversikt over databehandleravtaler meldt inn til personvernombud
- Ledelsens gjennomgang 2019. Alle byrådsavdelingene
- Reglement for akseptabel bruk av IKT
- Oversikt over gjennomførte nettbaserte kurs
- Dokumentasjon på gjennomførte DPIA
- Verktøy for vurdering av personvernkonsekvens
- Personvernerklæring for Bergen kommune
- Styrende dokument for digitalisering og IKT i Bergen kommune. Organisering, roller og ansvar
- IKT driftstjenesteavtale versjon 2.0, samt Bilag 1 *IKT styring*
- Byrådssak 1124/17. Digitalisering og innovasjon i Bergen kommune 2017-2020
- Byrådssak (saksnummer fremgår ikke/18). Digital fornyelse og iverksettelse av kanalstrategi i Bergen kommune
- Fullmakter for direktør for digitalisering og innovasjon konsern – delegert fra kommunaldirektør for HR, digitalisering og eiendom per 24. august 2017
- Overordnet ROS uke 11, 2019
- Oversikt over system, saksnummer, tilhørende byrådsavdeling og ev. enhet og navn på systemeier
- Utkast rapport: *Forvaltning av konsernansvar for informasjonssikkerhet.* Byrådsleders avdeling – seksjon for internkontroll.
- Tilbakemelding på rapport «forvaltning av konsernansvar informasjonssikkerhet». Fra SDI til seksjon for internkontroll. 18.10.2019.

- Diverse dokument og oversikter gjennom tilgang til Bergen kommunes intranett, BK prosjekt BK kvalitet.
- 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 4: Nettfiskeforsøk

Innhold

1.0 Innledning 3
2.0 Formål 3
3.0 Konklusjon 3
4.0 Anbefalinger 4
5.0 Vedlegg 1: Gjennomgang av resultater 5
5.1 Omfang og avgrensning 5
5.2 Analyseresultat 7
5.3 Metoder, verktøy m.m. 9

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».*

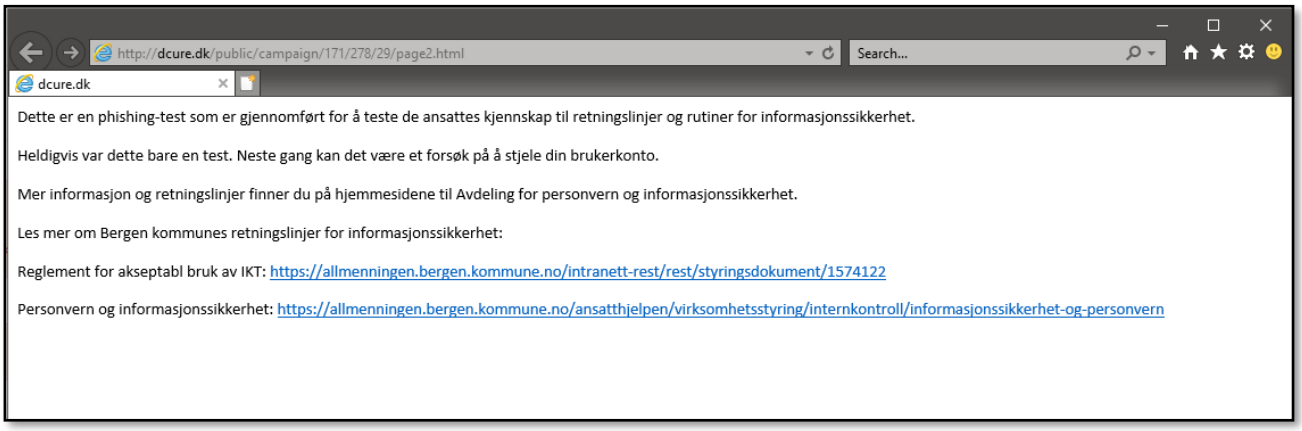
I e-posten ble de ansatte oppfordret til å klikke på en lenke for å besvare undersøkelsen. Lenken bestod av en unik URL generert for hver medarbeider, som gjør det mulig å spore hver enkelt medarbeiders besøk på nettsiden lenken førte til.

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.

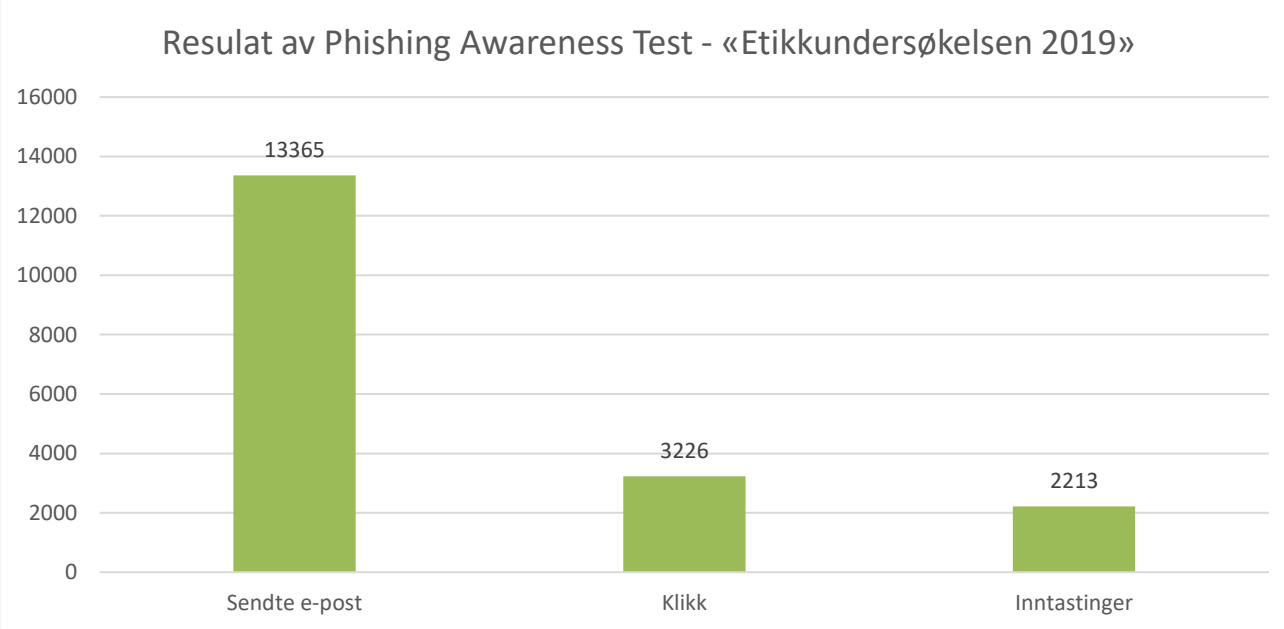
Utbyttet av det samlede angrepet bestod dermed av 2 213 passord med tilhørende e-post, noe som utgjør en **høy IT-sikkerhetsrisiko**.

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 5: Sikkerhetstester

Vedlegget er unntatt offentlighet etter offentlighetsloven § 24 tredje ledd.

Deloitte.