Rapport

MARKER KOMMUNE

07.09.2023

Forvaltningsrevisjon
IKT-sikkerhet

Innhold

1 SAMMENDRAG

Rapporten besvarer følgende problemstillinger:

Revisjonen har i denne forvaltningsrapporten vurdert hvorvidt Marker kommune har etablert en internkontroll knyttet til IKT-sikkerhet som følger krav og anbefalinger fra Digitaliseringsdirektoratet (Digdir) og Nasjonal sikkerhetsmyndighet (NSM), samt om kommunens ansatte kjenner til retningslinjer og rutiner på området.

Revisjonskriteriene i rapporten er utledet med bakgrunn i krav og anbefalinger fra Digdir og NSM innen digitalisering, nærmere bestemt de krav og anbefalinger som gjelder IKT-sikkerhet.

Revisjonens fremgangsmåte

En av målsetningene med forvaltningsrevisjonen har vært å kontrollere om kommunens arbeid med IKT-sikkerhet er i tråd med de krav og anbefalinger til informasjonssikkerhet som Digdir stiller på tidspunkt for revisjon. Dette gjelder blant annet krav til etablert internkontroll, bruk av protokoller for kommunikasjon på internett og på nettsteder, og bruk av kravspesifikasjon for PKI[1]. Videre gjelder det blant annet anbefalinger knyttet til NSMs grunnprinsipper for IKT-sikkerhet, støtte for protokoller for filoverføringer, og sikkerhetsanbefalinger for å redusere risiko for brudd på integritet ved oppslag i domenenavnsystemet, samt sikring av epost og kommunikasjonskanaler.

Den andre målsetningen har vært å kontrollere om kommunens ansatte har kjennskap til de retningslinjer og rutiner for IKT-sikkerhet som kommunen har etablert, og om de ansatte mener å ha fått tilstrekkelig opplæring og kunnskap på området.

For å svare ut problemstillingene har revisjonen gjennomgått sentrale dokumenter knyttet til internkontroll og IKT-sikkerhet, gjennomført intervjuer med nøkkelpersoner, samt sendt ut en spørreundersøkelse til ansatte i kommunen. Spørreundersøkelsen er gjennomført ved hjelp av Forms, et nettbasert verktøy for spørreundersøkelser.

Revisjonens funn og konklusjoner

Etter revisjonens vurdering følger Marker kommune i stor grad Digdir og NSM sine krav og anbefalinger for IKT-sikkerhet. Kommunen har flere dokumenter og prosedyrer som omhandler internkontroll og IKT-sikkerhet, og revisjonens inntrykk er at kommunen jobber aktivt med dette og har gjort mye godt arbeid for å styrke IKT-sikkerheten i kommunen. Undersøkelsen viser imidlertid også at det gjenstår noe arbeid før kommunen er i mål med å etablere et helhetlig internkontrollsystem på området.

Kommunen mangler enkelte sentrale rutiner på området og noen eksisterende rutiner er mangelfulle. De skriftlige rutinene for avvik er til dels motstridende og det er ikke definert hva som er et avvik i tilknytning til IKT-sikkerhet. Revisjonen har funnet at kommunen har utført risikovurderinger og ROS-analyser, men det fremkommer at funn fra disse ikke er fulgt opp eller dokumentert utført. Revisjonens konklusjon er at Marker kommune ikke har et helhetlig internkontrollsystem for IKT-sikkerhet per i dag og er av den oppfatning at IKT-sikkerheten i kommunen vil bli styrket dersom et mer helhetlig internkontrollsystem blir etablert.

[1] Public Key Infrastructure (PKI) – offentlig nøkkelkryptering

Når det gjelder ansattes kjennskap til retningslinjer og rutiner for IKT-sikkerhet har revisjonen funnet at kommunen har etablert noen tiltak for å øke ansattes kjennskap til disse, men at det likevel er manglende kjennskap blant en del ansatte knyttet til konkrete dokumenter/rutiner/retningslinjer. Kommunen har også iverksatt noe opplæring på området, men mange ansatte opplever at de får lite opplæring, og kommunen har heller ikke etablert en plan for opplæring på dette området.

Revisjonens anbefalinger

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

a) påse at den skriftlige rutinen for avvik oppdateres samt definere hva som er et avvik
b) påse at alle A-feil registreres som avvik samt definere hva som er en A-feil
c) påse at kommunens virksomheter kartlegger egen sårbarhet ved bortfall av EKOM-tjenester
d) sikre at kritisk utstyr har UPS
e) etablere planer for kommunikasjon/informasjonsformidling ved bortfall av EKOM
f) lage enhetlige tiltakskort for CIM-rapportering
g) påse at risikovurdering fremgår som del av «Sikkerhetshåndboka» eller internkontrollsystemet
h) dokumentere at kommunen har utført de 15 sikkerhetstiltakene med 1. prioritet jf. NSM
i) påse at varslingsrutine omfatter varsling til NSM samt vurdere behov for bistand
j) etablere en skriftlig rutine for hvordan kommunen skal gjennomføre opplæring
k) påse at opplæringen blir utført samt dokumentere dette
l) påse og dokumentere at alle ansatte har lest «Sikkerhetshåndboka» og vedlegget

2 MANDAT FOR FORVALTNINGSREVISJONEN

Revisjonen skal i henhold til kommunelovens § 24-2 (1) utføre forvaltningsrevisjon. Etter loven innebærer forvaltningsrevisjon å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets vedtak og forutsetninger. Østre Viken kommunerevisjon IKS gjennomfører forvaltningsrevisjon i tråd med god kommunal revisjonsskikk, som vil si å følge *Standard for forvaltningsrevisjon* (RSK 001) (NKRF[2], 2020). Dette innebærer blant annet at rapporten skal skille klart mellom innsamlede data (fakta) og revisjonens vurderinger. Det skal være en tydelig sammenheng mellom problemstillinger, faktaopplysninger[3], vurderinger, konklusjoner og eventuelle anbefalinger. Etter kommuneloven skal revisor rapportere resultatene av sin revisjon til kontrollutvalget.

Forvaltningsrevisjonen er gjennomført på bakgrunn av plan for forvaltningsrevisjon 2022-2024 vedtatt i kommunestyret i Marker kommune i sak 21/86 14. desember 2021.

Prosjektplan for gjennomføring av denne forvaltningsrevisjonen ble vedtatt i kontrollutvalget 16. februar 2023. Planen ble vedtatt i tråd med revisjonens forslag.

Forvaltningsrevisjonen er gjennomført etter vedtatt prosjektplan i tidsrommet februar – september 2023. Vi har gjennomført et oppstartsmøte med kommuneadministrasjonen slik at også administrasjonens innspill er tatt hensyn til.

Vi har kvalitetssikret faktagrunnlaget underveis, både gjennom verifisering av intervjuer og intern kvalitetssikring. I tillegg er rapportens faktaopplysninger i sin helhet verifisert av kommunen, slik at eventuelle feil eller misforståelser er rettet opp. Revisjonen avholdt avsluttende møte med administrasjonen 31. august 2023 hvor revisjonens vurderinger, konklusjoner og anbefalinger ble gjennomgått. I etterkant av møtet er rapporten sendt på høring til kommunedirektøren (se kapittel 6).

Forvaltningsrevisjonen er gjennomført av forvaltningsrevisor Dag Henriksen og oppdragsansvarlig revisor Casper Støten. Revisorenes habilitet og uavhengighet er vurdert opp mot kommunen og den undersøkte virksomheten, og revisjonen finner de habile til å utføre forvaltningsrevisjonen.

Revisor vil takke kontaktpersonen og andre som har deltatt for et godt samarbeid i forbindelse med gjennomføringen av forvaltningsrevisjonen.

Østre Viken kommunerevisjon IKS
Rolvsøy, 7. september 2023

Casper Støten (sign.)
oppdragsansvarlig revisor

Dag Henriksen (sign.)
utførende forvaltningsrevisor

[2] NKRF er en faglig interesseorganisasjon og et kompetanseorgan for kontroll og revisjon av kommunal/offentlig virksomhet.

[3] Fakta er en gjengivelse av informasjonen vi har fått tilgang til gjennom datainnsamlingen.

3 FREMGANGSMÅTE

3.1 Problemstillinger og avgrensninger

Rapporten besvarer følgende problemstillinger:

Problemstilling 1: Har Marker kommune etablert et internkontrollsystem for IKT-sikkerhet?
Problemstilling 2: Har kommunens ansatte kjennskap til rutiner for IKT-sikkerhet?

3.2 Om revisjonskriterier

I henhold til forskrift om kontrollutvalg og revisjon § 15 skal revisor fastsette revisjonskriterier for den enkelte forvaltningsrevisjon. Revisjonskriteriene er den objektive målestokk som setter revisor i stand til å gjøre vurderinger på de fleste områder uten å ha formell fagspesifikk kompetanse. Revisjonskriteriene og revisors kunnskap og erfaring innen forvaltningsrevisjonsmetodikk, gjør at revisor kan gjøre objektive og holdbare vurderinger.

Revisjonskriteriene etablerer den norm som de innsamlede dataene skal vurderes opp mot. I tillegg til dette skal revisjonskriteriene også gjøre det tydelig for den reviderte enhet hva de måles opp mot. Revisjonskriteriene klargjør også overfor folkevalgte, media og andre lesere av forvaltningsrevisjonen, hva revisors vurderinger bygger på. Dette vil gjøre det enklere å etterprøve revisors vurderinger. Revisjonskriteriene skal være relevante, konkrete og i samsvar med de kravene som gjelder for revidert enhet.

Revisjonskriterier fastsettes vanligvis med basis i en eller flere følgende kilder: lovverk, politiske vedtak og føringer, kommunens egne retningslinjer, anerkjent teori på området, eller andre sammenlignbare virksomheters løsninger og resultater.

3.3 Revisjonsmetoder

I henhold til god revisjonsskikk skal praksis eller tilstand innen det reviderte området beskrives i et omfang som i tilstrekkelig grad underbygger revisors vurderinger og konklusjoner. I denne forvaltningsrevisjonen har vi benyttet data fra ulike kilder, og brukt ulike metoder for innsamling av data, for å sikre et faktagrunnlag med høyest mulig grad av gyldighet og pålitelighet.

Utfordringer og begrensninger i rapportens faktagrunnlag beskrives nedenfor sammen med beskrivelsen av de ulike metodene som er benyttet. Vi tar også hensyn til metodens begrensninger i vurderingene.

I denne forvaltningsrevisjonen er informasjonen hentet inn gjennom bruk av følgende metoder:

- Dokumentanalyse
- Intervjuer
- Spørreundersøkelse

Dokumentanalyse

Vi har gjennomgått sentrale dokumenter på området. Blant annet har Sikkerhetshåndbok for informasjonssikkerheten, ROS-analyse IKT og rapport fra Sikkerhetsrevisjon 2021 vært sentrale for revisjonens undersøkelse. Dokumentene er oversendt fra kommunen. Fullstendig oversikt over dokumentene fremgår av kildehenvisningene i kapittel 8.

Intervjuer

Det er totalt gjennomført 2 intervjuer:
- Fungerende rådmann Vidar Østenby
- IT-konsulent

Begge intervjuene er verifisert. Det betyr at den som er intervjuet, har fått lese gjennom referatet fra intervjuet for å bekrefte at referatet er i overenstemmelse med det som ble sagt under intervjuet, og rette opp eventuelle misforståelser.

Spørreundersøkelse

Det er gjennomført en spørreundersøkelse blant kommunens ansatte. Undersøkelsen er gjennomført ved hjelp av det nettbaserte spørreundersøkelsesverktøyet Forms (Microsoft).

Spørreundersøkelsen ble sendt ut til kommunens ansatte som har tilgang til kommunens informasjonssystemer i sitt daglige arbeid. Undersøkelsen ble sendt til rundt 400 ulike e-postadresser, og det ble mottatt 141 svar. Det gir en svarprosent på 35,3 %. Dette er lavere enn ønskelig, men revisjonen vurderer likevel at spørreundersøkelsens resultater sammenstilt med funn fra øvrige kontrollhandlinger er tilstrekkelig for å gjøre pålitelige vurderinger.

Spørreundersøkelsen besto av 21 spørsmål. Målsettingen med spørreundersøkelsen var å få et inntrykk av de ansattes kjennskap til kommunens retningslinjer og rutiner for IKT-sikkerhet og personvern, og av hvor god opplæring innen informasjonssikkerhet de opplever å ha fått.

4 INTERNKONTROLLSYSTEM FOR IKT-SIKKERHET

Problemstilling 1: Har Marker kommune etablert et internkontrollsystem for IKT-sikkerhet?

4.1 Revisjonskriterier

Revisjonskriteriene er punktvis oppsummert nedenfor, og fremgår detaljert i kapittel 8.1 «Utledning av revisjonskriterier».

Kommunen skal ha etablert en tilstrekkelig god internkontroll på informasjonssikkerhetsområdet. Internkontrollsystemet skal også omhandle følgende punkter gjeldende for kommunens IKT-sikkerhet:
- ha planer og rutiner (sikkerhetstiltak) for å sikre beredskap
- gjennomføre risikovurderinger knyttet til IKT-sikkerhet
- ha rutiner for å varsle om IKT-sikkerhetshendelser
- ha vurdert behov for bistand ved IKT-sikkerhetshendelser
- bruke kravspesifikasjon for PKI ved anskaffelse av PKI-tjenester
- bruke IPv4 og IPv6 ved kommunikasjon på internett og vurdere om nytt IT-utstyr støtter dette
- bruke HTTPS på sine nettsteder

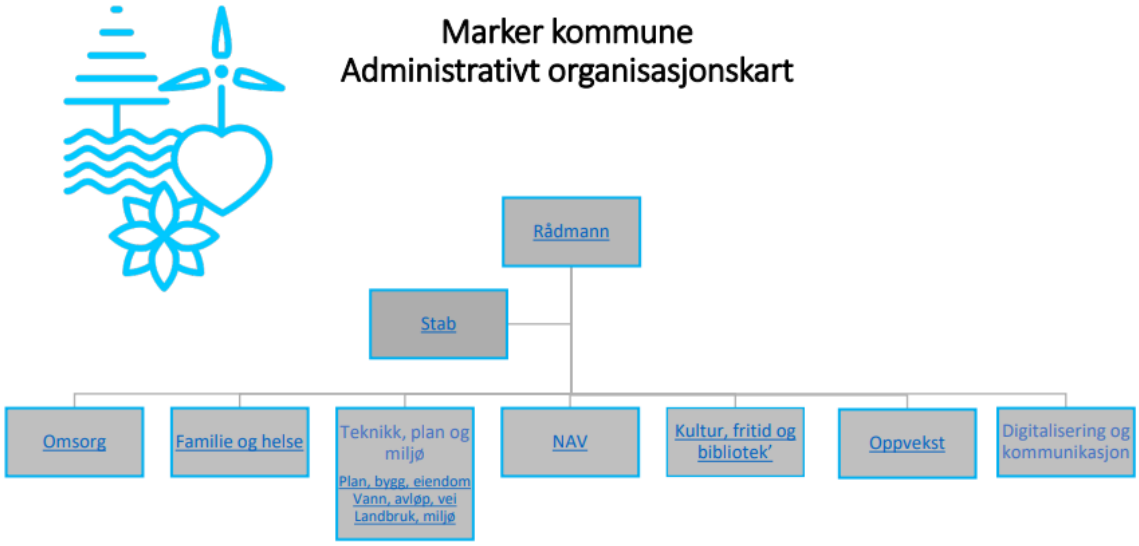
Kommunen bør:
- bruke NSM sine grunnprinsipper for IKT-sikkerhet
- bruke Digdirs «Interkontroll i praksis – informasjonssikkerhet» i arbeidet med internkontroll
- bruke DNSSEC for å redusere risikoen for brudd på integritet

- bruke DMARC for å motvirke falske avsendere av e-post
- bruke STARTTLS og SPF for transportsikring av e-post
- Kommunen bør støtte FTP som protokoll for filoverføring
- Kommunen bør bruke standarder fra Digdirs veiledning for bruk av VPN, for å sikre sine kommunikasjonskanaler

4.2 Datagrunnlag

4.2.1 Organisering

Marker kommune har organisert sin virksomhet i syv seksjoner for tjenestelevering, med en stab som ivaretar kommunens fellesfunksjoner.



Figur 1. Marker kommunes organisasjonskart

Marker er en liten kommune med omtrent 3600 innbyggere. Administrasjonen består av få nøkkelpersoner som er tildelt mange ulike roller og ansvar. Kommunen har omtrent 250 årsverk fordelt på rundt 400 stillinger. Marker kommune er i utgangspunktet en to-nivå kommune, hvor virksomhetslederne er organisert direkte under rådmannen, men hvor viktige oppgaver også er plassert i rådmannens ledergruppe og i staben. «Rådmann» refererer i organisasjonskartet over til rådmannens ledergruppe. Den består for det første av fungerende rådmann, som er stedfortreder for rådmann som er sykemeldt. Fungerende rådmann er også kommunalsjef Nærings- og utvikling samt at han også er kommunens sikkerhetsansvarlig. I tillegg sitter ytterligere to kommunalsjefer i ledergruppen, Kommunalsjef økonomi (økonomisjef) og Kommunalsjef HR (HR-sjef). Stab og støttefunksjoner består av næring, HR, spesialpedagogisk veileder, økonomikontor og kommuneoverlege. Økonomikontoret har fem ansatte og ledes av økonomisjefen. Hver av de syv virksomhetene ledes av virksomhetsledere, som har sin myndighet direkte delegert fra fungerende rådmann Vidar Østenby.

4.2.2 Internkontroll

Rådmannens ansvar for internkontroll etter kommuneloven § 25, er forankret i dokumentet «Sikkerhetshåndbok for informasjonssikkerheten i Marker kommune», hvor det også i kapittel 3.1 fremkommer at

rådmann har det overordnede, juridiske ansvar for informasjonssikkerheten i kommunen. Hver virksomhetsenhet har også et eget sikkerhetsansvar gjennom sine respektive ledere. Overordnet operativt ansvar for disse områdene er tillagt fungerende rådmann og kommunalsjef Vidar Østenby. Operativt ansvar innebærer å videreutvikle og overvåke arbeidet med informasjonssikkerhet og personvern i kommunen. Sikkerhetshåndboken ble utformet på bakgrunn av «Rapport fra Sikkerhetsrevisjon av fysiske, organisatoriske og systemtekniske sikkerhetsforhold inkl personvern i Marker kommune». Dette dokumentet fra sikkerhetsrevisjonen er datert til november 2022. Sikkerhetshåndboken revisjonen har fått oversendt er oppdatert i november 2022, og må regnes som kommunens styrende dokument for informasjonssikkerhet og internkontroll for IKT.

Som beskrevet i revisjonskriteriene skal kommunen ha etablert internkontroll på IKT-sikkerhetsområdet. Internkontrollen skal være basert på en vurdering/identifisering av relevante lov- og regelverk, herunder bør kommunen bruke NSMs grunnprinsipper blant annet:

- ha rutiner for å oppdage og fjerne kjente sårbarheter og trusler
- vurdere og klassifisere, kontrollere og håndtere, og evaluere og lære av hendelser

Videre er det beskrevet i revisjonskriteriene at kommunens internkontroll også bør være basert på Digdirs[4] «Internkontroll i praksis – informasjonssikkerhet» i arbeidet med internkontroll, konkretisert i følgende syv hovedpunkter:

- Ledelsens styring og oppfølging
- Vurdering av risiko
- Håndtering av risiko
- Overvåking og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling
- Kommunikasjon

Sikkerhetshåndboken inneholder blant annet definerte sikkerhetsmål og sikkerhetsstrategi. Videre er det i håndboken gjort bestemmelser knyttet til avvikshåndtering, hvor det fremgår i kapittel 1.3.1 at: «Bruk av IT-systemene skal skje i overensstemmelse med fastlagte rutiner og retningslinjer, og det er den enkelte medarbeiders ansvar å rapportere eventuelle avvik, for eksempel sikkerhetsbrudd, til nærmeste overordnede.» Sist i Sikkerhetsboken er vedlegget «Personvern og data-/informasjonssikkerhet i Marker kommune er også MITT ansvar som medarbeider». Dette er et egenerklæringsskjema som inneholder tretten punkter om IKT-sikkerhet som alle ansatte skal kjenne til. Fungerende rådmann forteller at ledelsen innimellom har gjennomganger av Sikkerhetshåndboken, og den inneholder utfordringsområder som er drøftet med virksomhetslederne. Blant annet skal alle ansatte fylle ut en egenerklæring på IKT-sikkerhet. Han forklarer at egenerklæringen også har en lesebekreftelse-funksjon som gjøre at man kan kontrollere om de ansatte har lest den. Kommunen har siden 2017 brukt TQM[5] (Total Quality Management) som ledelsessystem for internkontroll, rutiner og avviksbehandling blant annet, men revisjonen klarte ikke å se i TQM, eller på annen måte at det var mulig å se status for slik lesebekreftelse.

[4] Digdir – eller Digitaliseringsdirektoratets side om internkontroll

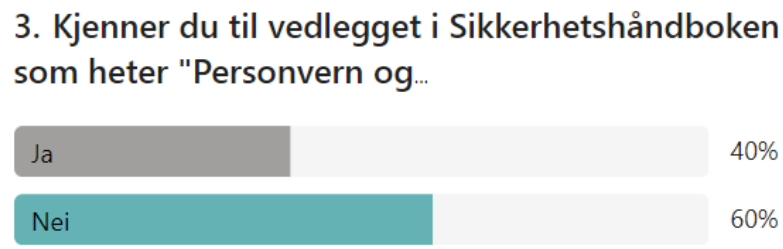
[5] TQM er et ledelsessystem

Slik det fremkommer av spørreundersøkelsen var det var 48 % som svarte at de kjenner til "Sikkerhetshåndbok for informasjonssikkerheten i Marker kommune".

Tabell 1. Spørreundersøkelsens spørsmål nr. 2

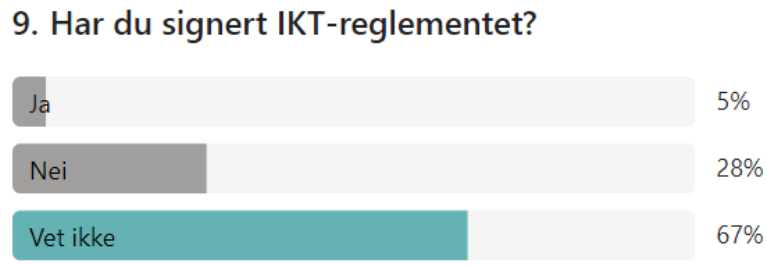
Videre svarte 40 % at de kjente til vedlegget i Sikkerhetshåndboken, "Personvern og data-/informasjonssikkerhet er også MITT ansvar", som omfatter egenerklæringen for signering.

Tabell 2. Spørreundersøkelsens spørsmål nr. 3



Ved spørsmål i spørreundersøkelsen svarer 5 % at de har signert IKT-reglementet.

Tabell 3. Spørreundersøkelsens spørsmål nr. 3



Videre fremgår det av spørreundersøkelsen at dersom de hadde opplevd avvik svarte 66 % av respondentene at de ville meldt inn avviket i TQM, mens 11 % svarte at de ville meldt avvik til nærmeste leder. Om de noen gang hadde meldt inn avvik knyttet til IKT-sikkerheten svarte 3 % at de hadde gjort det, og alle opplevde at avviket ble behandlet / lukket.

Fungerende rådmann sier om avvik at det er på to områder det kan være avvik. For det første er det avvik knyttet til at noe ikke fungerer. Da rapporteres det til Aspit[6], som er kommunens leverandør av IT-

[6] Aspit AS – leverandør av IT-drift og IT-sikkerhet

drift og IT-sikkerhet. Og så har kommunen TQM som avvikssystem som er mer formalisert, og rutinen for alle ansatte er at avvik skal meldes der. Slike avvik dreier seg gjerne om hva som er konsekvensene av at det har skjedd en svikt i systemet. Slike ting følges opp av kommunen i regi av TQM-programmet. Tilgangen, eller rettighetene til rådmann er overført til fungerende rådmann, og han forteller at systemet fortsatt ikke er helt optimalt – det hender at han får avviksmeldinger som handler om små avvik lokalt og som ikke er adressert riktig.

IT-konsulent med ansvar for IT-sikkerhet forteller at hvis det er en hendelse, om det er sikkerhet eller GDPR, kan dette meldes inn i kommunens kvalitetssystem TQM. Ved sikkerhetsbrudd kan alle ansatte melde inn avviket gjennom TQM, og alle har tilgang til det. TQM er og internkontrollsystemet kommunen benytter til IKT-sikkerhet, og det dekker ikke bare IKT. Man logger seg inn i TQM med Microsoft-kontoen. IT-konsulenten forteller at dette er noe de ansatte kjenner til, men han forteller også at for de to siste årene er det kun registrert ett avvik i systemet knyttet til IKT-sikkerhet. Han forklarer at det kan være vanskelig å vurdere om en hendelse er et avvik eller om det handler om behov for IT-support. Men hvis det gjelder for eksempel et bortfall av internett i hele kommunen så blir det regnet som et avvik. I virksomhet Omsorg regner man seks timers nedetid som et alvorlig avvik. Han forteller også at virksomhet Omsorg bruker avviksmeldingene veldig aktivt.

IT-konsulenten forteller at det utenom virksomhet Omsorg er veldig lite som meldes inn, og viser til TQM og at det er totalt tre registrerte avvik i systemet som går på IKT-sikkerhet. Han forklarer at det må være hendelser av en viss alvorlighetsgrad for at det skal regnes som et avvik. Det er fungerende rådmann som vanligvis skal lukke avviket, men det varierer fra sak til sak hvem som kan lukke. Videre opplever IT-konsulenten at det er unødvendig komplisert å finne fram i avvikssystemet i TQM. Revisjonen er blitt forevist den skriftlige rutinen som omhandler avvik. Rutinen er kalt «Prosedyre For Hendelsesmeldere i TQM» og ligger lagret i TQM.

Som grunnlag for kommunens informasjonssikkerhet og Sikkerhetshåndboken, har kommunen benyttet følgende lover/forskrift som alle berørte ledere og medarbeidere skal gjøres kjent med og følge det til enhver tid gjeldende lovverk:

- Personopplysningsloven (POL)
- EU/EØS-forordningen GDPR om vern av fysiske personer
- § 15 i Lov om helseregistre og behandling av helseopplysninger (Helseregisterloven)
- Kommuneloven
- Opplæringsloven
- Sikkerhetsloven
- Lov om arkiv
- Forskrift om internkontroll - Helse, Miljø, Sikkerhet (HMS)
- Arbeidsmiljøloven

4.2.3 Beredskap

Fungerende rådmann forteller at han er beredskapsansvarlig. Det er dermed han som er ansvarlig for at kommunen følger opp Sikkerhetslovens § 4-3. Plikt til å gjennomføre sikkerhetstiltak og øvelser. Så har Virksomhetsikkerhetsforskriften krav om beredskap i: § 14. Grunnsikringstiltak, påbyggingstiltak og tiltak for skadebegrensning og gjenopprettelse. Beredskapsarbeidet i Marker kommune bygger på en ROS-analyse fra 2016 som omhandler bortfall av tjenester, og kommunen har en beredskapsplan fra omtrent samme tiden. Revisjonen har også fått presentert dokumentet «IT-beredskapsplan avd. Drift» som del av «Beredskapsplan – Marker kommune». Dette er en varslingsrutine for Aspit AS og Marker

kommune. Det fremgår av denne rutinen at alvorlige hendelser (A-feil) som rammer hele organisasjonen, eller store deler av den skal varsles. Det fremgår ingen eksempler eller beskrivelser i rutinen på hva en A-feil kan være. Fungerende rådmann forteller at kommunen hadde et bortfall av internett i romjulen. Da ba de om en kartlegging i virksomhetene av hvordan de kan håndtere svikt. Dette er virksomhetsspesifikt. Virksomhet Omsorg tar utskrifter ganske ofte i tilfelle det skulle bli bortfall. Det samme gjelder vann/avløp og andre. Han sier videre at virksomhetene skal kunne fungere noen dager, men det skal ikke vare så mye lengre før det blir problematisk. Revisjonen fant ikke at det var registrert avvik knyttet til bortfall av internett romjulen 2022.

En ny overordnet ROS-analyse utarbeidet av Rambøll AS[7] ble behandlet i kommunestyret 27. april 2023. Bortfall av kritisk infrastruktur har nå blitt et tema for kommunen, og de har i 2023 sammen med Statsforvalteren og andre kommuner testet samhandlingen når kritisk infrastruktur faller bort. Trusler mot eller bortfall av Ekom-tjenester (EKOM elektronisk kommunikasjon) er i ny overordnet ROS-analyse vurdert til å ha høy sannsynlighet og store konsekvenser. Slik det fremgår av denne ROS-analysen har ikke kommunens forskjellige virksomheter kartlagt egen sårbarhet ved bortfall av EKOM-tjenester. Kommunen har heller ikke sikret at kritisk utstyr som håndterer sentralbord, alarmer og kritiske varslingssystemer har UPS (Uninterruptible Power Supply). Videre fremgår det at kommunen mangler planer for kommunikasjon/informasjonsformidling ved bortfall av EKOM, og at kommunen bør vurdere/kartlegge behov og tilgjengelighet på kommunikasjonsutstyr som kan benyttes ved bortfall av EKOM, for eksempel satellittelefon, nødnettstilknytning o.l.

Når det gjelder implementering av endringer eller nye systemer sier fungerende rådmann at ledende IKT-konsulent er flink til å kjøre tester. Det er også utført en såkalt phishing[8]-test blant alle ansatte og 10 % lot seg lure til å klikke på en «ondsinnet lenke». Han forteller videre at han har opplevd løsepengeepost, men at dette var før skylagringen ble innført. Hendelsen berørte lokalt lagrede data, hvor det ble brukt en minnepinne som forårsaket sikkerhetsbruddet. Det var et omfattende arbeide for kommunen å rette dette opp. Revisjonen kunne ikke finne at dette var innmeldt som et avvik, men fungerende rådmann forteller at dette var før TQM var tatt i bruk.

Fungerende rådmann forteller at det meste er skybasert nå og at kommunen ikke har noen datamaskiner som er rigget for å håndtere bortfall av nett, men at om så skulle skje så har de beredskapssystemet på papir, og noe lagret lokalt. Han forteller videre at han satt i koordinatorgruppen i DigiViken, og at han der så at Marker kommune har ligget i forkant på mange av de systemene som handler om IKT-sikkerhet. Men han legger til at det er en potensiell sårbarhet som ligger i at det er kun to personer som jobber med dette i kommunen. Han legger til at dette er grunnen til at kommunen har etablert virksomheten Digitalisering og kommunikasjon, og han mener at kommunen har omstrukturert seg for å ta høyde for arbeidet med informasjonssikkerhet. Virksomhetsleder har kompetanse på prosjektstyring og vil komme tilbake med viktige satsninger. Kommunen har også ansatt en som skal jobbe prosjektbasert med informasjonssikkerhet og lignende.

Fungerende rådmann forteller at beredskapsrutinen kan hentes frem i TQM-systemet kommunen benytter til internkontrollsystem og avvikssystem, og at de også er tilknyttet CIM[9] hvor de loggfører større hendelser. Han forklarer at kommunen jobber med å lage enhetlige tiltakskort, noe som gjøres i samarbeid med Indre Østfold kommune – og at det er hensiktsmessig at kommunene har noenlunde like tiltakskort, men at dette ikke er på plass enda. Han legger til at beredskap er et tema som ofte er forsømt i mindre kommuner, men at planene har blitt mer samkjørte etter pandemien. Han forteller at CIM-

[7] Rambøll er et globalt arkitektur-, ingeniør- og konsulentfirma

[8] Phishing – hvor en angriper forsøker å lure noen til å utføre en handling

[9] CIM - verktøy for informasjonsdeling i forbindelse med ulykker og uønskede hendelser

rapporteringen er i bruk, og at dette fungerer greit, men at det er litt vanskelig å integrere ulike nivåer internt i kommunen, så det brukes primært på overordnet nivå.

4.2.4 Risikovurderinger

Risikovurdering på IKT-sikkerhetsområdet er ikke lagt inn i Sikkerhetshåndboken, og revisjonen har ikke sett noen skriftlig rutine eller føringer for hvordan arbeidet med risikovurdering på området skal foregå. Men det fremgår av Sikkerhetshåndboken at kommunens sikkerhetsansvarlig skal påse at «det ved behov gjennomføres nødvendige risikovurderinger og eventuelt andre egenkontroller».

Revisjonen har fått oversendt ROS-analyser for IKT-sikkerhet over Aspit og over IT-avdelingen fra henholdsvis mai og september 2022. Risikoanalysen er gjort i et risikostyringsverktøy. Revisjonen har også fått dokumentet «Nordlo Sårbarhetsanalyse MS365 Marker kommune» fra februar 2023. Dette er en sårbarhetsanalyse av Microsoft 365 plattformen, hvor hensikten er å kontrollere innstillingene i Markers Microsoft 365-plattform med fokus på fire områder: Tenantsikkerhet, identitet, e-postsikkerhet og databeskyttelse. Resultatet av Nordlo-analysen viser at Microsoft 365-tenanten er konfigurert i henhold til beste praksis i ganske stor grad, men noen funksjoner burde justeres for å øke sikkerheten. Når det gjelder implementering av endringer eller nye systemer sier IT-konsulenten at kommunen tester lite selv, men at Aspit gjør det da det er et krav som ligger hos dem som leverandør. Marker kommune har også tatt en risikovurdering i 2020 over alle «NSMs[10] Grunnprinsipper for IKT-sikkerhet». Disse består i 118 sikkerhetstiltak og vurderingene kommunen gjorde resulterte i 15 tiltak i kategorien 1. prioritet. Revisjonen fant ikke en egen oversikt hvor det fremgår hvilke tiltak kommunen har gjort med 15 sikkerhetstiltakene med 1. prioritet.

Ut over dette har kommunen avtale med HelseCERT[11] som gjør en skanning hver fjortende dag. Da prøver de å bryte seg inn i systemet, og så lager de en rapport på hvordan det har gått. IT-konsulenten legger til at kommunen ikke har en fullverdig overvåkning, og at det er et ønske om at kommunen skal anskaffe seg SOC/SIEM[12], som er bestilt og skal leveres ved årsskiftet. Han forteller at det nylig er funnet en svakhet i systemet som ble fulgt opp. Rapportene fra HelseCERT kommer til han på epost, men disse blir ikke lagret i noe system eller sammenstilt på noen måte.

4.2.5 Varslingsrutiner og bistand

Det er krav iht. sikkerhetsloven § 4-5 at virksomheter plikter å varsle NSM ved visse forhold. Varsling om uønskede hendelser til NSM er en lovpålagt plikt. Som nevnt over har kommunen en varslingsrutine. Denne har overskriften «Varslingsrutine Marker kommune». Det fremgår av denne rutinen at alvorlige hendelser (A-feil) som rammer hele organisasjonen, eller store deler av den skal varsles. Slik det fremgår av rutinen er det Aspit som skal varsles, dermed omhandler ikke rutinen varsling til NSM. Det fremgår heller ikke noe punkt i rutinen som sier noe om hvorvidt kommunen har vurdert behov for bistand ved IKT-sikkerhetshendelser. Det fremgår ingen eksempler eller beskrivelser i rutinen på hva en A-feil kan være. Revisjonen fant heller ikke om det ble varslet til Aspit for eksempel ved nevnte bortfall av internett romjulen 2022, eller hvordan hendelsen ble fulgt opp.

[10] NSM – Nasjonal sikkerhetsmyndighet og grunnprinsipper for IKT-sikkerhet

[11] HelseCERT er helse- og omsorgssektorens nasjonale senter for cybersikkerhet.

[12] SOC/SIEM er verktøy som fokuserer på trusselovervåking og kvalifisering av hendelser.

4.2.6 PKI og internettprotokoller

Det fremkommer i intervjuet med IT-konsulenten at kravet fra Digdir til PKI (offentlig nøkkelkryptering)[13] er helt nødvendig å følge, og at det ikke finnes noe system som fungerer uten dette. IT-konsulenten forteller videre at kommunen selv ikke har utarbeidet noen egen kravspesifikasjon for anskaffelser av PKI-tjenester, men bruker de standarder og anbefalinger gitt av leverandørene. Revisjonen har fått oversendt en generell kravspesifikasjon kommunen benytter. Kravene som følger av eIDAS-forordningen og selvdeklarasjonsforskriften er teknologinøytrale, og stiller ikke krav om PKI-teknologi. Det er derfor ikke lenger nødvendig å oppfylle Kravspesifikasjon for PKI i offentlig sektor for å levere eID-ordninger på høyeste sikkerhetsnivå.

IT-konsulenten sier at hos kommunen skal alt være sikkert så de bruker Fiks-plattformen[14] fra KS, og det går aldri noe utenom PKI. Det er alltid en tjenesteleverandør eller en programvare som setter opp kommunens løsninger, og de har full kontroll på type sertifikater som er nødvendige for at løsningen skal fungere. Han mener også at utstedere som Buypass informerer godt.

Når det gjelder internettprotokoller og nettverksstandard forteller IT-konsulenten at kommunen kun bruker IP versjon 4 (IPv4) som nettverksprotokoll, og at en omlegging til nyeste versjon IPv6[15] vil kreve fullstendig omlegging av infrastrukturen. Forskriften om IT-standarder i offentlig forvaltning presiserer at IPv4 og IPv6 er grunnleggende protokoller for kommunikasjon på internett. Alt IT-utstyr som det offentlige anskaffer bør ha støtte for IPv4 og IPv6. Forskrift § 12, siste ledd, presiserer dette ytterligere, og sier at nye interne nett og løsninger i offentlige virksomheter skal ha støtte for IPv6, men at det er tillatt å støtte IPv4 i tillegg.

HTTPS er overføring av nett-trafikk over en sikker forbindelse. Ved å bruke krypteringsprotokollen Transport Layer Security (TLS) kan klienten verifisere identiteten til tjenesteleverandøren, og nett-trafikken kan overføres kryptert – som gjør det uleselig for uvedkommende under transporten.

Revisjonskriteriet om HTTPS[16] bygger på kravet som kom i oktober 2021 om sikker datakommunikasjon fra offentlige nettsteder, og som er spesifisert i forskrift om IT-standarder i offentlig sektor § 11. IT-konsulenten forteller i intervju i april at kommunen kun bruker HTTPS som kommunikasjonsprotokoll på kommunens nettsider, og at de for noen få uker faset ut den eldre TLS 1,1 til fordel for TLS[17] 1,2 som krypteringsprotokoll.

Slik det fremgår av NSM sin veileder «Grunnprinsipper for IKT-sikkerhet» bør kommunen også bruke standard for sikker bruk av domenenavn. Mer konkret er DNSSEC (DNS Security Extensions) en sikkerhetsmekanisme som legges inn i domenenavnsystemet. IT-konsulenten forteller at kommunen ikke har dette på hjemmesidene, fordi leverandøren foreløpig ikke tilbyr det. Han legger til at kommunen har sertifikater, men at kommunen ikke har internettsider som er veldig sårbare. Han forteller at leverandøren er GP Nett (Halden dataservice), og at det er de som DNS-leverandør og som står for dette. Kommunen er medlem av DigiViken hvor de kan drøfte slike løsninger. Han forteller at domenet «kommune.no» har DNSSEC, men ikke noe ut over det.

[13] PKI (Public Key Infrastructure) er en sikker krypteringsmetode for digital kommunikasjon.

[14] Fiks-plattformen til KS har digitale fellesløsninger kommunen kan ta i bruk.

[15] Les mer om internettprotokollene IPv4 og IPv6 i denne artikkelen hos one.com

[16] HTTPS er sikrere enn HTTP som kommunikasjonsprotokoll mot WWW, les mer på Wikipedia

[17] Transport Layer Security (TLS), tidligere kalt Secure Sockets Layer (SSL), er en kryptografisk protokoll.

4.2.7 FTP, VPN og sikring av e-post

FTP står for File Transfer Protocol, og er en nettverksprotokoll som brukes for å overføre filer fra klient til server, man kan si at FTP er språket som brukes mellom to datamaskiner for å sende filer over internett eller nettverket. Selv om Digdir fortsatt anbefaler støtte for FTP er ikke denne protokollen særlig aktuell lengre. For det første ble den ikke designet for å være en sikker protokoll, og for det andre er behovet for den i praksis borte da kommunen benytter seg av skytjenester i stor grad. IT-konsulenten forteller i intervju at kommunen heller benytter den videreutviklede SFTP som krypteringsteknikk.

Digdir anbefaler også VPN som standard for sikring av kommunikasjonskanaler. VPN står for et virtuelt privat nettverk. Med et VPN-program kobles man til en ekstern server via en sikker «tunnel» som opprettes, og all trafikken gå gjennom denne serveren før den når ut til internett. Informasjonen krypteres, man kan få endret IP-adressen og anonymisert brukeren. Men bruken av VPN i jobbsammenheng er ikke lenger like aktuell som tidligere fordi det nå fins ulike Citrix-løsninger og sikrere autentiseringsmetoder. IT-konsulenten forteller i intervju at kommunen ikke bruker VPN, men at de kan bruke en Citrix-løsning for eksempel til hjemmekontorløsninger tilpasset virksomhet Omsorg. Ellers er de tilknyttet skyen med tofaktorautentisering.

Når det gjelder sikring av e-post har revisjonen fokusert på to av NSM sine «Grunnprinsipper for IKT-sikkerhet». Det ene grunnprinsippet er DMARC, anbefalt standard for å motvirke falske avsendere av e-post. Det andre grunnprinsippet er beskyttelsesmekanismen som sørger for autentisering av eposttjenere og konfidensialitetssikring - StartTLS for sikring av e-post. IT-konsulenten forteller at kommunen bruker kryptert e-post og presiserer at det også er kryptering mellom servere, for eksempel med NAV. Han forklarer at for avsendere sikres epost ved hjelp av DMARC, SPF (Sender Policy Framework) og/eller DKIM (Domain Keys Identified Mail). Ved overføring brukes StartTLS. Dette er en kommando som informerer epostserveren om at epostklienten ønsker å oppgradere fra usikker til sikker kobling ved bruk av TLS eller SSL. I tillegg kan også SPF brukes for å spesifisere hvilke eposttjenere som er autorisert til å sende e-post på vegne av et gitt domene. Kommunen bruker eksterne aktører som tester sikkerheten for DMARC og StartTLS. Disse er HelseCERT, et nasjonalt beskyttelsesprogram som tester robustheten til offentlige IKT-systemer, og Nordlo som tester kommunens sikkerhetsnivå i Microsoftplattformen.

4.3 Vurderinger

Slik det fremgår av revisjonskriteriene er det 7 «skal» punkter og 7 «bør» punkter revisjonen har undersøkt opp mot kommunens internkontrollsystem for IKT-sikkerhet.

4.3.1 Internkontroll

Det er dokumentet «Sikkerhetshåndboka» samt enkelte rutiner i TQM som må regnes som kommunens internkontrollsystem på informasjonssikkerhetsområdet. Ut over Sikkerhetshåndboka har ikke kommunen et eget dokument med tittel «Internkontrollsystem» eller lignende for IKT-sikkerhetsområdet.

Det fremgår av dokumentets kapittel 1.3 Sikkerhetsstrategi, hvordan kommunen organiserer internkontrollsystem og rutiner på området:
«*Disse rutiner og prinsipper er i overensstemmelse med kravene til internkontroll i POL inkl. GDPR og annet relevant, nasjonalt sikkerhetsregelverk, og skal sikre at personvernet og sikkerhetsarbeidet for øvrig i kommunen blir en kontinuerlig prosess - ivaretatt på en systematisk og dokumentert måte.*

Internkontroll representerer kommunens kvalitetssystem, styringssystem eller ledelsessystem for etterlevelse av regelverk. Internkontroll er med andre ord ***ledelsens*** *verktøy for å kunne ivareta sitt ansvar og etterleve lover og forskrifter inkl. personvernregelverket, og* ***medarbeidernes*** *verktøy for å kunne utføre sine oppgaver på en forsvarlig og sikker måte.*
Tiltak knyttet til kommunens internkontroll skal stadig forbedres, dokumenteres og oppdateres ved behov.»

Det er rådmann som har ansvar for internkontrollen, og har det overordnede, juridiske ansvar for informasjonssikkerheten eller datasikkerheten i kommunen. Det er Østenby som er fungerende rådmann og som også har overordnet operativt ansvar for å videreutvikle og overvåke arbeidet med informasjonssikkerhet og personvern i kommunen. Østenby er også kommunalsjef for beredskap, næring og utvikling og han er beredskapsansvarlig.

Når det gjelder kommunens retningslinjer knyttet til avvikshåndtering, fremgår det i Sikkerhetshåndboka kapittel 1.3.1 at: «det er den enkelte medarbeiders ansvar å rapportere eventuelle avvik, for eksempel sikkerhetsbrudd, til nærmeste overordnede.» Kommunen har i tillegg den skriftlige rutinen «Prosedyre For Hendelsesmeldere i TQM» som omhandler avvik og er lagret i TQM. Her fremgår det at alle ansatte skal melde avvik i TQM. Revisjonen er av den oppfatning at kommunens rutiner for å melde avvik ikke er konsekvente da ansatte blir bedt om å melde avvik to ulike steder.

Fungerende rådmann fortalte at enkelte avvik ikke blir adressert riktig i TQM. IT-konsulenten fortalte at for de to siste årene er det kun registrert ett avvik i systemet som omhandler IKT-sikkerhet, og at det kan være vanskelig å vurdere om det er et avvik eller om det handler om support. Oppsummert er det revisjonens oppfatning at kommunen har to forskjellige rutiner for hvordan avvik skal meldes, noe som kan føre til forvirring blant de ansatte, samt fare for at avvik ikke blir meldt og heller ikke fulgt opp. Videre har vi sett at enkelte avvik adresseres feil og noen avvik ikke har blitt registrert. Vi finner heller ikke at det fremgår av rutinene at kommunen har definert hva som er et avvik.

4.3.2 Beredskap

Beredskapsarbeidet i Marker kommune bygger på en ROS-analyse fra 2016 som omhandler bortfall av tjenester, og kommunen har en beredskapsplan fra omtrent samme tiden. Ny overordnet ROS-analyse ble behandlet i kommunestyret i april 2023, og som nevnt over er det Østenby som er beredskapsansvarlig.

Revisjonen har vurdert dokumentet «IT-beredskapsplan avd. Drift» som del av «Beredskapsplan – Marker kommune», som er en varslingsrutine for Aspit AS og Marker kommune. Det fremgår ingen eksempler i rutinen på hva en A-feil kan være, men kommunen hadde bortfall av internett romjulen 2022, noe som regnes som en A-feil, men revisjonen kunne ikke finne at dette var et registrert avvik.

Kommunen utførte en ROS-analyse i 2023 hvor det viser seg at kommunens forskjellige virksomheter ikke har kartlagt egen sårbarhet ved bortfall av EKOM-tjenester. Kommunen har heller ikke sikret at kritisk utstyr som håndterer sentralbord, alarmer og kritiske varslingssystemer har UPS (Uninterruptible Power Supply). Videre fremgår det at kommunen mangler planer for kommunikasjon/informasjonsformidling ved bortfall av EKOM, og at kommunen bør vurdere/kartlegge behov og tilgjengelighet på kommunikasjonsutstyr som kan benyttes ved bortfall av EKOM, for eksempel satellittelefon, nødnettstilknytning o.l. Kommunen har vært utsatt for «løsepengevirus» og hadde et omfattende arbeid med å rette dette opp. Etter dette har det meste blitt skybasert og sikrere, men hendelsen viser at kritiske systemer i kommunen har blitt satt ut av spill. Revisjonen er av den oppfatning at beredskapsarbeidet med kritisk infrastruktur og EKOM bør styrkes.

Videre er kommunen tilknyttet CIM hvor større hendelser skal loggføres. CIM-rapportering er i bruk på overordnet nivå, men kommunen er ikke i mål med å lage enhetlige tiltakskort.

Revisjonen er av den oppfatning at kommunens beredskapsansvar innen «hverdagshendelser» er på plass. Dette handler om robusthet i kommunens tjenester og funksjoner, forebyggende aktiviteter og evne til å respondere, bl.a. hos nød- og redningstjenestene (grunnberedskap). Kommunen har beredskapsansvar innen flere ulike tjenester og funksjoner, slik som eks. IKT-sikkerhet, vannforsyning og helse- og omsorgstjenester. I tillegg til helhetlig ROS for kommunen har slike tjenester og funksjoner også egne lov- og forskriftskrav til ROS-analyser for sin virksomhet. Den kommunale beredskapsplikten skal bidra til å samordne, supplere og skape sammenhenger mellom alle de områdene (funksjoner og tjenester) som er en del av samfunnssikkerhet og beredskap på lokalt nivå.

4.3.3 Risikovurderinger

Revisjonen finner at kommunen har vurdert risiko for området i ROS-analyser fra mai og september 2022, en «Nordlo Sårbarhetsanalyse» fra 2023 samt en overordnet ROS-analyse 2023. Risikovurdering skal være en del av kommunens internkontroll, men risikovurdering på IKT-sikkerhetsområdet er ikke lagt inn i Sikkerhetshåndboken, og revisjonen har ikke sett noen skriftlig rutine eller føringer for hvordan arbeidet med risikovurdering på området skal foregå eller hvor ofte dette skal utføres. Revisjonen er av den oppfatning at internkontrollsystemet vedrørende risikovurderinger er for svakt da vi kun finner nevnt at «det ved behov gjennomføres nødvendige risikovurderinger og eventuelt andre egenkontroller».

Slik det fremgår av NSM sin veileder «Grunnprinsipper for IKT-sikkerhet», kan manglende prosesser for risikovurdering føre til at ledelsen ikke får tilstrekkelig informasjon til å prioritere og styre virksomhetens sikkerhetsarbeid. Prinsippet med å kartlegge styringsstrukturer, leveranser og understøttende systemer, handler om at virksomheten må identifisere, prioritere og beskytte sine viktigste leveranser. Mangelfull oversikt kan føre til at enkelte, mindre viktige deler av IKT-systemet kan være godt sikret, mens andre mer vesentlige deler er eksponert og sårbart for angrep.

Marker kommune har også tatt en risikovurdering i 2020 over alle «NSMs[18] Grunnprinsipper for IKT-sikkerhet». Disse består i 118 sikkerhetstiltak som ble vurdert mot kommunens systemer. Resultatet fra denne risikovurderingen var at kommunen hadde 15 tiltak i kategorien 1. prioritet. Revisjonen fant ikke en oversikt hvor det fremkommer hvilken fremdrift kommunen har med å utføre disse 15 sikkerhetstiltakene med 1. prioritet. Revisjonen er av den oppfatning at kommunen bør utføre de 15 tiltakene og dokumentere arbeidet.

4.3.4 Varslingsrutiner og bistand

Kommunen plikter å varsle NSM ved visse forhold. Kommunen har en varslingsrutine, men denne oppgir kun at Aspit skal varsles, og dermed omhandler ikke rutinen varsling til NSM. Det fremgår heller ikke noe punkt i rutinen som sier noe om å vurdere behov for bistand ved IKT-sikkerhetshendelser.

4.3.5 PKI og internettprotokoller

Revisjonen er av den oppfatning at kommunen følger kravet fra Digdir når det gjelder PKI (offentlig nøkkelkryptering) og sikker krypteringsmetode for digital kommunikasjon. Sikker kommunikasjon over kommunens IKT-systemer er basert på de standarder og anbefalinger gitt av leverandørene.

[18] NSM – Nasjonal sikkerhetsmyndighet og grunnprinsipper for IKT-sikkerhet

Når det gjelder internettprotokoller og nettverksprotokoll sier IT-konsulenten at kommunens nettverksutstyr og programvare støtter IPv6, men dersom kommunen skal innføre kommunikasjon på internett med nyeste versjon IPv6[19] så vil det kreve fullstendig omlegging av infrastrukturen. Slik det fremgår av forskriften om IT-standarder i offentlig forvaltning, presiseres det at IPv4 og IPv6 er grunnleggende protokoller for kommunikasjon på internett og at alt IT-utstyr som det offentlige anskaffer bør ha støtte for IPv4 og IPv6. Forskriftens § 12, siste ledd, presiserer dette ytterligere, og sier at nye interne nett og løsninger i offentlige virksomheter skal ha støtte for IPv6, men at det er tillatt å støtte IPv4 i tillegg. Revisjonens har tolket anbefalingen og forskriften slik at det er en sterk anmodning til offentlige virksomheter til å bruke IPv6 for kommunikasjon på internett, men at det ikke er et absolutt krav. Revisjonen er derfor av den oppfatning at kommunen bør vurdere å begynne og bruke IPv6 for kommunikasjon på internett, men finner ikke tilstrekkelig grunnlag for å komme med en konkret anbefaling om dette på nåværende tidspunkt.

IT-konsulenten har forklart at kommunen bruker HTTPS som kommunikasjonsprotokoll på kommunens nettsider. Revisjonen har også manuelt kontrollert mange av kommunens nettsider for å se om de bruker HTTPS. På bakgrunn av dette er det revisjonens vurdering at kravet om sikker datakommunikasjon over kommunens nettsted er ivaretatt.

Revisjonen har vurdert revisjonskriteriet om at kommunen bør bruke DNSSEC for å redusere risikoen for brudd på integritet. Dette er en metode som sikrer at du kommer til den adressen du vil nå. IT-konsulenten forteller at kommunens nett-leverandør er GP Nett (Halden dataservice), og at det er de som DNS-leverandør og som står for dette. Han forteller at domenet «kommune.no» har DNSSEC, men ikke noe ut over det. Resultat fra Nordlo[20] viser også de har vurdert konfigureringen i kommunens offentlige DNS. Revisjonen har på bakgrunn av dette vurdert at kommunens nett tar høyde for dette grunnprinsippet for IKT-sikkerhet.

4.3.6 FTP, VPN og sikring av e-post

Nasjonal sikkerhetsmyndighet (NSM) sin veileder «Grunnprinsipper for IKT-sikkerhet» beskriver hva en virksomhet bør gjøre for å sikre et IKT-system, og FTP og VPN er blant anbefalte løsninger. Kommunen bruker hverken FTP eller VPN, og revisjonen er av den oppfatning at selv om NSM fortsatt anbefaler støtte for disse er de ikke særlig aktuell lengre, særlig etter omlegging av mange systemer til sky.

Slik det fremgår av revisjonskriteriene bør kommunen bruke DMARC og StartTLS for sikring av e-post. IT-konsulenten har inngående forklart revisjonen hvordan kommunens systemer tar høyde for NSM sine grunnprinsipper for sikring av e-post. Revisjonen har også sett på resultater fra HelseCERT, et nasjonalt beskyttelsesprogram som tester robustheten til offentlige IKT-systemer, der de har testet DMARC og StartTLS i kommunens system. Det foreligger også gode testresultater fra Nordlo som viser at kommunens sikkerhetsnivå på dette området i Microsoftplattformen er tilfredsstillende. Revisjonen vurderer det slik at disse to grunnprinsippene for sikring av e-post er ivaretatt av kommunen.

[19] Les mer om internettprotokollene IPv4 og IPv6 i denne artikkelen hos one.com

[20] Nordlo er en bedrift som jobber med sikring av IT- og skytjenester, se hjemmesiden.

4.4 Konklusjon og anbefalinger

Kommunen har flere dokumenter og prosedyrer som omhandler internkontroll og informasjonssikkerhet, og revisjonens inntrykk er at kommunen jobber aktivt med informasjonssikkerhet. Etter revisjonens vurdering følger Marker kommune i stor grad blant annet Digdir og NSM sine krav og anbefalinger gjeldende digitalisering i sitt informasjonssikkerhetsarbeid.

Revisjonens konklusjon er likevel at Marker kommune ikke har et helhetlig internkontrollsystem for IKT-sikkerhet. Revisjonen er av den oppfatning at IKT-sikkerheten i kommunen vil bli styrket dersom et mer helhetlig internkontrollsystem blir etablert. Vi har funnet enkelte forbedringsområder knyttet til dette som har resultert i anbefalingene gjengitt nedenfor.

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

- påse at den skriftlige rutinen for avvik oppdateres samt definere hva som er et avvik
- påse at alle A-feil registreres som avvik samt definere hva som er en A-feil
- påse at kommunens virksomheter kartlegger egen sårbarhet ved bortfall av EKOM-tjenester
- sikre at kritisk utstyr har UPS
- etablere planer for kommunikasjon/informasjonsformidling ved bortfall av EKOM
- lage enhetlige tiltakskort for CIM-rapportering
- påse at risikovurdering fremgår som del av «Sikkerhetshåndboka» eller internkontrollsystemet
- dokumentere at kommunen har utført de 15 sikkerhetstiltakene med 1. prioritet jf. NSM
- påse at varslingsrutine omfatter varsling til NSM samt vurdere behov for bistand

5 RUTINER FOR IKT-SIKKERHET

Problemstilling 2: Har kommunens ansatte kjennskap til rutiner for IKT-sikkerhet?

5.1 Revisjonskriterier

- De ansatte har fått opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av IKT-systemer
- De ansatte skal kjenne til kommunens egne rutiner og prosedyrer for IKT-sikkerhet
- Det gjennomføres kompetansetiltak for medarbeiderne for å styrke IKT-sikkerheten
- De ansatte har undertegnet en taushetserklæring ved inngåelse av arbeidsforholdet

5.2 Datagrunnlag

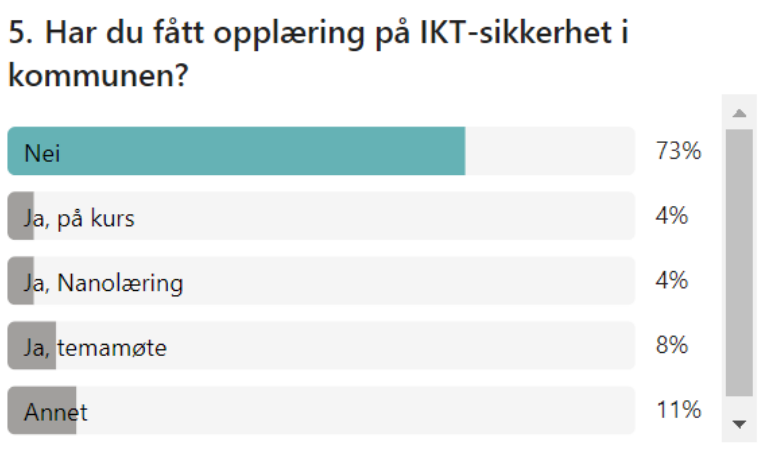
5.2.1 Opplæring

Kommunens reglement for IKT-sikkerhet er i prinsippet dokumentet «Sikkerhetshåndboken» fra november 2022. Sikkerhetshåndboken har et kapittel kalt «Sikkerhetsmål». Her fremgår det at sikringstiltak kan være knyttet til opplæring, og at sikkerhetstiltakene skal sørge for at alle ledere og medarbeidere i kommunen får nødvendig opplæring i alle sikkerhetsrelaterte forhold. Videre er det vedtatt i kapittelet «Fast ansatt personell og vikarer med tidsbegrenset arbeid» at medarbeidere på alle nivåer skal gjennomgå opplæring i bruk av IKT og i informasjonssikkerhet. IT-konsulenten forklarer i intervju med revisjonen at opplæring for kommunens ansatte når det gjelder IKT-sikkerhet er basert i hver enkelt virksomhet. Han forteller at kommunen har brukt noen nano-kurs, men at det mangler en opplæringsplan i kommunen og at det ikke finnes dokumentasjon på gjennomført opplæring eller kursing, eller plan for fremtidig opplæring når det gjelder IKT-sikkerhet.

Revisjonen undersøkte vha. en spørreundersøkelse om kommunens ansatte blant annet har fått opplæring i bruk av IKT og om de har kjennskap til rutiner for IKT-sikkerhet. Spørreundersøkelsen ble sendt til ansatte i Marker kommune og 141 respondenter har besvart. Undersøkelsen var anonym.

Flere av spørsmålene i spørreundersøkelsen handlet om ansattes opplæring innen IKT-sikkerhet. 85 % svarte at de har fått informasjon om IKT-sikkerhet på jobb. Slik det fremgår av tabell 4 svarte 27 % at de hadde fått opplæring på IKT-sikkerhet. 4 % av disse svarte at de har hatt nanolæring. Av spørsmål nr. 8 fremgår det at 32 % opplever at de «har fått tilstrekkelig informasjon/opplæring på IKT-sikkerhet».

Tabell 4. Spørreundersøkelsens spørsmål nr. 5



5.2.2 IKT-reglement

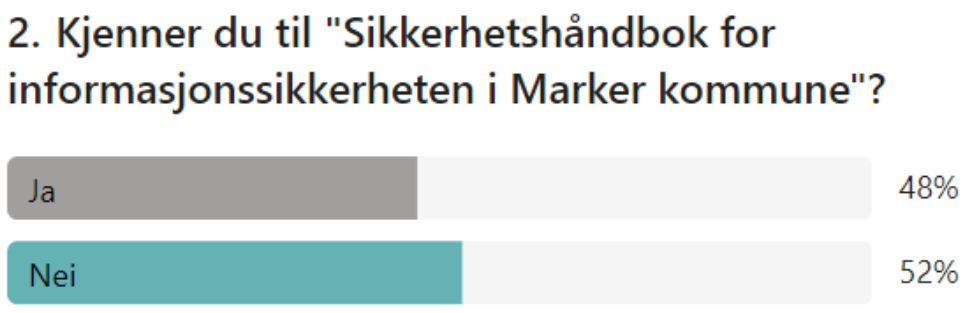
Kommunens IKT reglement gjelder for all bruk av Marker kommunes IKT-tjenester. Reglementet fastslår at med IKT-tjenester menes datamaskiner og IKT-systemer, sluttbrukerutstyr, nettverk, programmer, data mv. som kommunen stiller til disposisjon, eller andres maskiner og systemer som man får tilgang til gjennom slike ressurser. Reglementet gjelder også for privat utstyr så lenge det er koblet til Marker kommunes nettverk. IT-konsulenten forteller at det i utgangspunktet er virksomhetslederne som er ansvarlig for å informere sine ansatte om rutinene for IKT-sikkerhet.

Sikkerhetshåndboken som ble utformet på bakgrunn av «Rapport fra Sikkerhetsrevisjon av fysiske, organisatoriske og systemtekniske sikkerhetsforhold inkl personvern i Marker kommune» må regnes som kommunens styrende dokument for informasjonssikkerhet og internkontroll for IKT. Sikkerhetshåndboken inneholder blant annet definerte sikkerhetsmål og sikkerhetsstrategi. Videre er det i håndboken gjort bestemmelser knyttet til avvikshåndtering, hvor det fremgår i kapittel 1.3.1 at: «Bruk av IT-systemene skal skje i overensstemmelse med fastlagte rutiner og retningslinjer, og det er den enkelte medarbeiders ansvar å rapportere eventuelle avvik, for eksempel sikkerhetsbrudd, til nærmeste overordnede.» Sist i Sikkerhetsboken er vedlegget «Personvern og data-/informasjonssikkerhet i Marker kommune er også MITT ansvar som medarbeider». Dette er et egenerklæringsskjema som inneholder tretten punkter om IKT-sikkerhet som alle ansatte skal kjenne til.

IT-konsulenten sier videre at av alle kommunens virksomheter har virksomhet Omsorg vært veldig flinke til å følge opp med hensyn til IKT-sikkerhet. Han sier at han ikke vet konkret hvordan det informeres ut til de ansatte i virksomhetene, men at alle må lese Sikkerhetshåndboka. Det er lesekontroll på dokumentet i TQM, og det registreres i systemet når den ansatte har lest det, forklarer han.

Flere av spørsmålene i spørreundersøkelsen dreier seg om hvorvidt kommunens ansatte har kjennskap til kommunens reglement for IKT-sikkerhet. Det fremgår at 48 % av de som svarte på spørreundersøkelsen kjenner til Sikkerhetshåndboken, og at mesteparten av disse har vært ansatt i kommunen i mer enn to år.

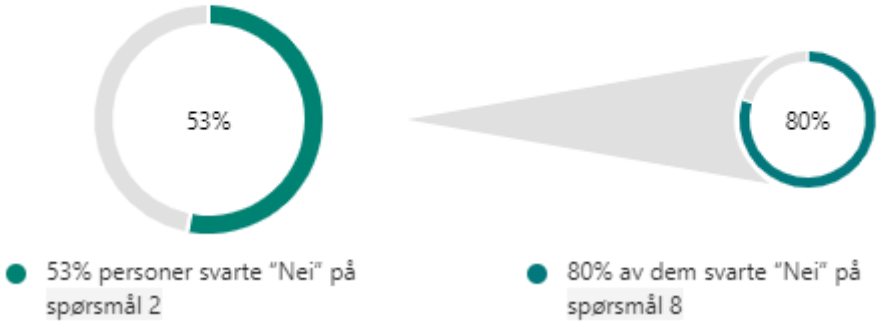
Tabell 5. Spørreundersøkelsens spørsmål nr. 2: Kjenner du til "Sikkerhetshåndbok for informasjonssikkerheten i Marker kommune"?



Blant de 53 % som svarte at de ikke kjenner til Sikkerhetshåndboken, svarer 80 % i spørsmål nr. 8 at de ikke opplever å ha fått tilstrekkelig informasjon/opplæring på IKT-sikkerhet.

Tabell 6. Spørreundersøkelsens spørsmål nr. 2 om innsikt i hvorvidt de som ikke kjenner til Sikkerhetshåndboken opplever og ha fått IKT-opplæring.

53% av personer svarte **Nei** på dette spørsmålet, og mesteparten svarte "**Nei**" på spørsmål 8.



På spørsmål om de kjenner til vedlegget i Sikkerhetshåndboken som heter "Personvern og data-/informasjonssikkerhet er også MITT ansvar" svarer 40 % ja. Dette vedlegget er ifølge fungerende rådmann en egenerklæring for signering av alle ansatte. Som vist i kapittel 4.2.2 Internkontroll, svarer 5 % at de har signert, mens 67 % ikke vet om de har signert IKT-reglementet. Revisjonen ser at dette spørsmålet kan være uheldig formulert, da IKT-reglementet og vedlegget og egenerklæringen "Personvern og data-/informasjonssikkerhet er også MITT ansvar" nødvendigvis ikke oppfattes som det samme. Likevel er det 60 % som svarer at de ikke kjenner til vedlegget. Revisjonen fant ikke i TQM at det fremgikk hvor mange som hadde lest Sikkerhetshåndboka, eller om vedlegget, egenerklæringen for signering, faktisk skal signeres av de ansatte, da det ikke står presisert skriftlig. Fungerende rådmann sier at alle ansatte signerer en taushetserklæring ved ansettelsen. Det fremgår også av Sikkerhetshåndboken i avsnitt «3.3.6 Taushetsplikt» at kommunen har utarbeidet et skjema som skal signeres.

5.2.3 Styrking av IKT-sikkerheten

NSM viser til sikkerhetsloven med forskrifter i sin «Veileder i personellsikkerhet», hvor bestemmelser knyttet til taushetserklæring og kompetanse fremgår. Styrking av IKT-sikkerheten ved gjennomføring av kompetansetiltak er pålagt en virksomhet etter § 7 i virksomhetsikkerhetsforskriften. Datatilsynet har i sin veileder om interkontroll og informasjonssikkerhet presisert at «Brukerne bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle risikoer». Revisjonen er ikke presentert noen rutiner for opplæring eller kompetanseheving, planer for kursing eller opplæring eller dokumentasjon på gjennomført opplæring eller kursing når det gjelder IKT-sikkerhet. IT-konsulenten opplyser revisjonen om at opplæring på IKT er basert i hver enkelt virksomhet. Det er sendt ut jevnlige informasjonsskriv, og kommunen har brukt noen nano-kurs. Videre oppgir IT-konsulenten at det mangler en opplæringsplan. Ledelsen må også ta stilling til det, det må komme litt ovenfra sier han, det er viktig at en slik plan blir forankret i kommunens ledelse. Videre forteller IT-konsulenten at kommunen ikke har noen plan for fremtidig opplæring når det gjelder IKT-sikkerhet.

Slik det fremgår av spørreundersøkelsen svarer 32 % (45 respondenter) at de opplever og ha fått tilstrekkelig informasjon/opplæring på IKT-sikkerhet, mens 68 % (96 respondenter) svarer nei på dette spørsmålet.

Tabell 7. Spørreundersøkelsens spørsmål nr. 8

8. Opplever du at du har fått tilstrekkelig informasjon/opplæring på IKT-sikkerhet?

Flere detaljer Innblikk

Ja	45
Nei	96

Videre i spørreundersøkelsen var det fokus på personvern. På spørsmål om de er kjent med reglene for lagring og bruk av personopplysninger i spørsmål 10, svarer 87 % (122 respondenter) at de er godt kjent – eller litt kjent med reglene.

Tabell 8. Spørreundersøkelsens spørsmål nr. 10

10. Lagring og bruk av personopplysninger, er du kjent med reglene for det?

Flere detaljer Innblikk

Jeg er godt kjent med de	42
Jeg er litt kjent med de	80
Jeg kjenner ikke til de reglene	19

Videre ble det i spørsmål 11, stilt spørsmål om de mener at alle ansatte i kommunen behandler personopplysninger iht. reglementet. Her svarte 21 % at de tror det, mens 79 % (112 respondenter) er usikker på eller tviler på at alle ansatte i kommunen behandler personopplysninger korrekt.

Tabell 9. Spørreundersøkelsens spørsmål 11

11. Mener du at alle ansatte i kommunen behandler personopplysninger iht. reglementet?

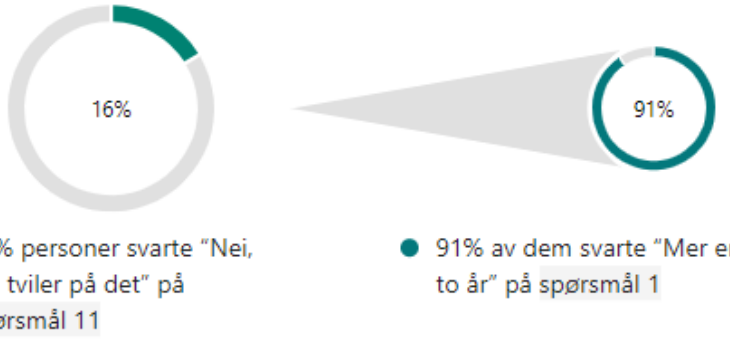
Flere detaljer Innblikk

Ja, jeg mener det	29
Jeg er usikker på det	90
Nei, jeg tviler på det	22

Blant de 16 % som svarer at de tviler på dette, er 91 % ansatt i mer enn to år.

Tabell 10. Innsikt i spørsmål 11 viser at de aller fleste som svarer nei, har vært ansatt i mer enn to år.

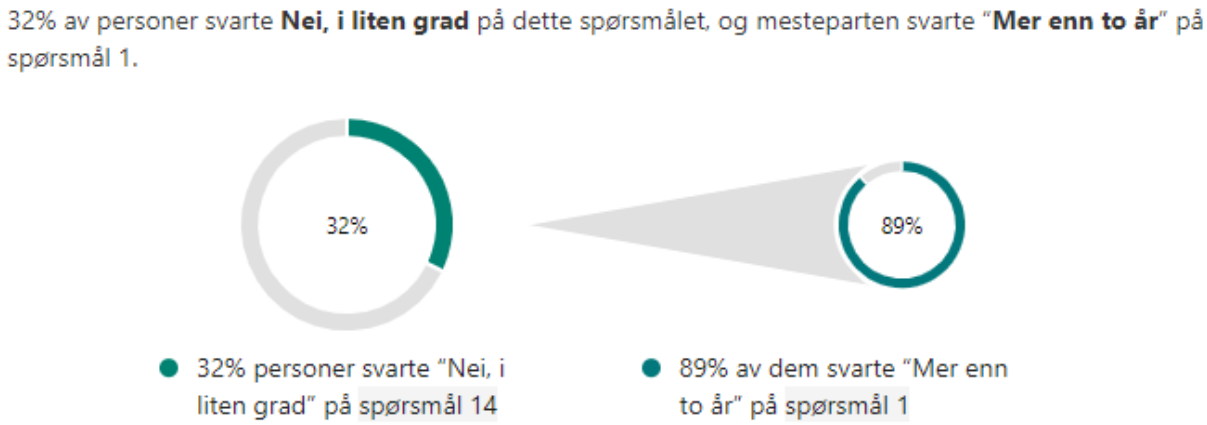
16% av personer svarte **Nei, jeg tviler på det** på dette spørsmålet, og mesteparten svarte "**Mer enn to år**" på spørsmål 1.



Videre fremgår det av spørreundersøkelsen at 3 % (4 respondenter) sier de har oppgitt sitt brukernavn og passord for sin kommune-login til noen andre. IT-konsulenten forteller at avdelingen nylig gjorde en «Spam-test» til ansatte der 7 av ca. 130 stykker lot seg lure til å oppgi brukernavn og passord.

Deretter var det i spørsmål nr. 14 fokus på om deres leder er opptatt av IKT-sikkerhet. Spørreundersøkelsen viste at 25 % av respondentene mener deres leder i stor grad er opptatt av IKT-sikkerhet, mens 32 % mente deres leder i liten grad er opptatt av dette. Blant de 32 % som mente leder i liten grad er opptatt av IKT-sikkerhet har 89 % vært ansatt i mer enn to år, og 75 % kjenner ikke til Sikkerhetshåndboken.

Tabell 11. Innsikt i spørreundersøkelsens spørsmål nr. 14. De aller fleste som mener deres leder er lite opptatt av IKT-sikkerhet er ansatt mer enn to år.



Av de 141 som svarte på spørreundersøkelsen er det 24 % som benytter hjemmekontor, og 94 % av disse sier at de alltid ivaretar sikkerheten på hjemmekontoret.

Videre fremgår det av spørreundersøkelsen i spørsmål nr. 20 at det er 13 % (17 respondenter) som bruker jobb-epostadressen til private formål. Det fremgår heller ikke av Sikkerhetshåndboken noe om bruk av jobb-epostadressen i privat sammenheng.

Tabell 12. Spørreundersøkelsens spørsmål nr. 20

5.3 Vurderinger

For at kommunens arbeid med informasjonssikkerhet skal bli en suksess, er det avgjørende at de ansatte får opplæring, og at de kjenner til de dokumenter og retningslinjer som kommunen har på området.

5.3.1 Opplæring

Slik det fremgår av «Sikkerhetshåndboka» skal alle ansatte gjennomgå opplæring i bruk av IKT og i informasjonssikkerhet. Revisjonen vurderer det slik at kommunen har brukt noe nano-kurs, men at det mangler en opplæringsplan i kommunen og at det ikke finnes dokumentasjon på gjennomført opplæring eller kursing, eller plan for fremtidig opplæring når det gjelder IKT-sikkerhet. Slik det fremgår av spørreundersøkelsen har kun 27 % svart at de har fått opplæring innen IKT-sikkerhet. På bakgrunn av dette er det revisjonens oppfatning at opplæringen i kommunen innen IKT-sikkerhet er mangelfull.

5.3.2 IKT-reglement

Det blir opplyst om at alle ansatte må lese «Sikkerhetsboka» og at det er lesekontroll på dette i TQM. Sist i Sikkerhetsboken er vedlegget «Personvern og data-/informasjonssikkerhet i Marker kommune er også MITT ansvar som medarbeider». Dette er et egenerklæringsskjema som inneholder 13 punkter om IKT-sikkerhet som alle ansatte skal kjenne til, og det var 48 % som svarte i spørreundersøkelsen at de kjente til «Sikkerhetshåndboka» og 40 % kjente til vedlegget. Revisjonens vurdering er at det er mange ansatte som ikke kjenner til IKT-reglementet og at kommunen har en jobb å gjøre i å styrke de ansattes kjennskap til IKT-reglementet og dermed også IKT-sikkerheten i kommunen.

5.3.3 Styrking av IKT-sikkerheten

Revisjonen er av den oppfatning av at det mangler rutiner for opplæring og kompetanseheving, planer for kursing og opplæring samt at det mangler dokumentasjon på gjennomført opplæring og kursing når det gjelder IKT-sikkerhet. Det fremkommer av spørreundersøkelsen at 32 % opplever og ha fått tilstrekkelig informasjon/opplæring på IKT-sikkerhet. Det fremkommer også at 7 ansatte i en nylig test lot seg lure til å oppgi brukernavn og passord, noe revisjonen mener er et høyt tall og kritisk for sikkerheten.

Styrking av IKT-sikkerheten ved gjennomføring av kompetansetiltak er pålagt en virksomhet etter § 7 i virksomhetsikkerhetsforskriften. Det fremgår videre av NSM i sin «Veileder i personellsikkerhet» bestemmelser knyttet til taushetserklæring og kompetanse. Revisjonen har fått bekreftet at alle ansatte signerer en taushetserklæring ved ansettelsen. Det fremgår også av Sikkerhetshåndboken i avsnitt «3.3.6 Taushetsplikt». Men slik det fremgår av spørreundersøkelsen har kommunen en jobb å gjøre når det gjelder kompetansetiltak for de ansatte for å styrke IKT-sikkerheten i kommunen.

5.4 Konklusjon og anbefalinger

Etter revisjonens vurdering har kommunen etablert noe opplæring samt noen tiltak som er egnet til å sikre ansattes kjennskap til retningslinjer og rutiner for IKT-sikkerhet. Revisjonens vurdering er likevel at Marker kommune i liten grad bruker ressurser på dette, og det viser seg at det er manglende kjennskap til dokumenter/rutiner/retningslinjer blant de ansatte. Revisjonens konklusjon blir da at det er mange ansatte som ikke har kjennskap til rutiner for IKT-sikkerhet.

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

- etablere en skriftlig rutine for hvordan kommunen skal gjennomføre opplæring
- påse at opplæringen blir utført samt dokumentere dette
- påse og dokumentere at alle ansatte har lest «Sikkerhetshåndboka» og vedlegget

6 KOMMUNEDIREKTØRENS UTTALELSE

Revisjonen oversendte forvaltningsrevisjonsrapporten til kommunedirektør for uttalelse den 01.09.2023.

Kommunedirektøren v/ kommunalsjef Vidar Østenby opplyste i e-post til revisjonen datert 07.09.2023 at kommunen ikke har kommentarer til rapporten.

7 KILDER

- Sikkerhetsloven, Lovdata
- eForvaltningsforskriften, Lovdata
- Forskrift om IT-standarder i offentlig forvaltning, Lovdata
- Digitaliseringsrundskrivet H2021-5, rundskriv fra Kommunal- og distriktsdepartementet
- Digitaliseringsdirektoratet Digdir (2022)
    - Referansekatalogen for IT-standarder.
    - Internkontroll i praksis – informasjonssikkerhet
- Nasjonal sikkerhetsmyndighet NSM (2022)
    - Grunnprinsipper for IKT-sikkerhet 2.0

Dokumenter fra Marker kommune:

- Organisasjonskart
- Sikkerhetshåndboka
- ROS-analyser
- Programoversikt
- Backup plan
- Kravspesifikasjon ved kjøp av PKI
- Avtale om driftstjenester
- Prosedyre For Hendelsesmeldere i TQM
- Rapport ra sikkerhetsrevisjon (2021)
- Varslingsrutiner
- HelseCERT Marker

8 VEDLEGG

8.1 Utledning av revisjonskriterier

Problemstilling 1
Har Marker kommune etablert et internkontrollsystem for IKT-sikkerhet?

IKT-sikkerhet omhandler både sikring mot hendelser som skyldes ondsinnede handlinger, og sikring mot hendelser som skyldes systemfeil og brukerfeil. I 2019 vedtok regjeringen en digitaliseringsstrategi for offentlig sektor for perioden 2019-2025. Retningen for arbeidet med digitalisering av offentlige tjenester er i tråd med føringene i Meld. St. 27 (2015-2016). Det fremkommer av strategien at ivaretakelse av personvern og informasjonssikkerhet er avgjørende for at offentlig sektor skal lykkes med digitaliseringsarbeidet. Videre at digitaliseringen krever gjennomgripende endringer i måten offentlig sektor utfører sine oppgaver på, og dermed også hvordan man sikrer og forvalter dokumentasjon. Ambisjonen om økt digitalisering betyr at styrking av personvern og informasjonssikkerhet blir stadig viktigere.

Regjeringen er øverste organ i sentralforvaltningen og ansvarlig overfor Stortinget, både når det gjelder saksforberedelser og gjennomføring av Stortingets vedtak. Departementene skal sørge for å gjennomføre vedtatt politikk, ofte gjennom ytre etater som direktoratene. Ifølge sikkerhetsloven er departementene ansvarlig for forebyggende sikkerhetsarbeid innenfor sine ansvarsområder.[21]
Det følger av eForvaltningsforskriftens § 15 om internkontroll på informasjonssikkerhetsområdet at 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.

Videre står det at forvaltningsorganet skal ha en interkontroll (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, og det organet departementet peker ut skal gi anbefalinger på området.

I digitaliseringsrundskrivet[22] fra Kommunal- og distriktsdepartementet (KDD), punkt 1.4 om oppfølging av informasjonssikkerheten, fremkommer det at KDD har pekt ut **Digitaliseringsdirektoratet (Digdir)** til det organ som skal gi anbefalinger om internkontroll (styring og kontroll) på informasjonssikkerhetsområdet, jf. eForvaltningsforskriften § 15. Digdir har utviklet en veileder som understøtter virksomhetsledelsens arbeid med helhetlig internkontroll, blant annet ved å hjelpe virksomheten til å identifisere plikter etter annet regelverk, som personvernforordningen.

Digdir ble formelt opprettet 1. januar 2020. Direktoratet har følgende hovedfunksjoner:

- Bidra til utvikling og gjennomføring av regjeringa sin IKT-politikk.
- Premissgiver for digitalisering og helskapt informasjonsforvaltning.
- Premissgiver for innovasjon i offentlig sektor, og et særlig ansvar som tilrettelegger for godt samspill mellom aktører på feltet.
- Koordinering av tverrgående digitaliseringstiltak.
- Strategisk planlegging og videreutvikling av en helskapt digital infrastruktur for offentlig sektor.
- Samordner og pådriver i offentlig sektors arbeide med forebyggende informasjonssikkerhet.

[21] Sikkerhetsloven § 2-1, se Lovdata.

[22] Digitaliseringsrundskrivet er en sammenstilling av pålegg og anbefalinger om digitalisering i offentlig sektor.

- Forvalte og utvikle klart språk.
- Utvikling av digitale tjenester for innbyggere, kommuner og næringsliv.
- Drift og forvaltning av felleskomponenter og fellesløsninger.
- Tilsyn for universell utforming av IKT.

Digdir beskriver arbeidet med informasjonssikkerhet som at det handler om å sikre informasjonsbehandling som inngår i oppgaver og tjenester[23]. Videre at det handler om å:

- Sikre informasjonssystemene som benyttes – inkludert digitale tjenester, IKT-systemer og komponenter som inngår i IKT-systemer
- Tilrettelegge arbeidsoppgaver (prosesser) slik at det er enkelt for mennesker å utføre oppgavene sine med god sikkerhet
- Sikre tilstrekkelig kompetanse hos de som utfører oppgaver for virksomheten og å jobbe for en kultur som understøtter arbeidet med informasjonssikkerhet

Som det fremkommer på Digdirs hjemmeside er det vanlig å si at informasjonssikkerhet handler om å sikre at informasjon i alle former:

- Ikke blir kjent for uvedkommende (konfidensialitet)
- Ikke blir endret utilsiktet eller av uvedkommende (integritet)
- Er tilgjengelig ved behov (tilgjengelighet)

Digdir har sammenstilt en oversikt over krav og anbefalinger som gjelder ved digitaliseringsarbeid i offentlig forvaltning. Knyttet til informasjonssikkerhet finner vi **fire krav**, som alle er forankret i forskrift om IT-standarder i offentlig forvaltning. De fire kravene er som følger:

1. **Bruk grunnleggende protokoller for kommunikasjon på internett.**
   IPv4 og IPv6 er grunnleggende protokoller for kommunikasjon på internett. Alt IT-utstyr som det offentlige anskaffer bør ha støtte for IPv4 og IPv6.

Forskrift om IT-standarder i offentlig forvaltning § 12, siste ledd, presiserer dette ytterligere, og sier at nye interne nett og løsninger i offentlige virksomheter skal ha støtte for IPv6, men at det er tillatt å støtte IPv4 i tillegg.

2. **Bruk internkontroll på informasjonssikkerhetsområdet.**

Referansekatalogen for IT-standarder inneholder obligatoriske og anbefalte standarder som gjelder for internkontroll/styringssystem/ledelsessystem på informasjonssikkerhetsområdet.

Det er obligatorisk for forvaltningsorgan som benytter elektronisk kommunikasjon å ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. eForvaltningsforskriften § 15 «Internkontroll på informasjonssikkerhetsområdet» sier følgende i 1.-3. ledd:

«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

[23] Digdir – om arbeid med IKT-sikkerhet hos offentlig virksomhet.

bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området. Omfang og innretning på internkontrollen skal være tilpasset risiko.»

Det er anbefalt å basere seg på gjeldende versjon av ISO/IEC 27001[24]. Digdirs veiledning **«Internkontroll i praksis – informasjonssikkerhet»** er basert på denne standarden, og konkretiserer de mest sentrale delene av standarden til syv hovedaktiviteter. Det er anbefalt å bruke veiledningsmateriellet som referanse og støtte ved analyse av status, og ved etablering og forbedring av internkontroll på informasjonssikkerhetsområdet. De syv hovedaktivitetene er:

- **Ledelsens styring og oppfølging.** Ledelsen er ansvarlig for å etablere tilstrekkelig styring og kontroll i virksomheten. For å lede virksomheten på en god måte, er ledelsen avhengig av tilstrekkelig styring på informasjonssikkerhetsområdet. Det oppnås gjennom etablering og oppfølging av et systematisk arbeid med styring av informasjonssikkerhet i hele virksomheten.
- **Vurdering av risiko** – vurderingene kan gjelde hele virksomheten på strategisk nivå, enkelte oppgaver eller tjenester, eller spesifikke informasjonssystemer eller deler av disse.
- **Håndtering av risiko.** Grovt sett finnes fire hovedalternativer for håndtering av risiko; unngå, dele, redusere, akseptere. Sikkerhetstiltak etableres og forvaltes for å redusere risiko, gjennom å redusere konsekvenser av uønskede hendelser eller sannsynligheten for at de inntreffer. Risikoen kan også deles eller aksepteres.
- **Overvåking og hendelseshåndtering.** Virksomheten må forberede seg på at uønskede hendelser, avvik og informasjonssikkerhetsbrudd kan forekomme. Som en del av risikohåndteringen blir det derfor etablert tiltak som har som formål å oppdage informasonssikkerhetshendinger, håndtere dem og redusere konsekvensene ved slike hendinger.
- **Måling, evaluering og revisjon.** Formålet er at ledere på alle nivåer skal få bedre kunnskap om tilstanden på sitt ansvarsområde. Det må systematisk gjøres vurderinger om sikkerhetstiltakene fungerer, om regelverk blir etterlevd, og om internkontrollarbeidet i virksomheten blir gjennomført som planlagt. Dette gjøres gjennom ulike kombinasjoner av målinger, undersøkinger, evalueringer og revisjoner.
- **Kompetanse- og kulturutvikling.** Både kompetanse og kultur er en avgjørende del av arbeidet med styring av informasjonssikkerhet. Ansatte med ulike roller må ha nødvendig kunnskap, vite hvorfor informasjonssikkerhet er viktig, og ha grunnleggende forståelse for hva det handler om.
- **Kommunikasjon.** God kommunikasjon, både skriftlig og muntlig, er en forutsetning for god styring og kontroll. Dokumentasjon er en viktig del av dette, og virksomheten må ha tydelige føringer for hvordan kommunikasjon og dokumentasjon skal foregå.

Digdir presiserer at lov- og regelverkskrav kan være mer omfattende enn krav og anbefalinger i nevnte standard. Virksomhetene må derfor, som en del av arbeidet, identifisere og etterleve de lov- og regelverkskrav som gjelder for dem.

3. Bruk kravspesifikasjon for PKI ved anskaffelse av PKI-tjenester.

Public Key Infrastructure (PKI) er en overordnet, funksjonell kravspesifikasjon for anskaffelse av PKI, og blir brukt i forbindelse med elektronisk kommunikasjon med og i offentlig sektor. Offentlig nøkkelkryptering (PKI) handler om elektronisk identifisering og signatur, samt kryptering for hemmelighold. Dette er en nyttig, og ofte nødvendig, funksjonalitet når offentlig sektor tilbyr digitale tjenester til sine innbyggere. Det er viktig at brukeren er identifisert, slik at det er sikkert at vedkommende er den den utgir seg for å være – slik at sensitiv informasjon ikke gis ut til feil person, eller kommer på avveie. For kommunen er det obligatorisk å bruke «Kravspesifikasjon for PKI i offentlig sektor versjon 2.0» ved:

- Anskaffelse av PKI-tjenester i markedet til bruk i elektronisk kommunikasjon mellom offentlige virksomheter og med innbyggere eller næringsliv.
- Elektronisk signering i forbindelse med tinglysning, jf. Forskrift om prøveprosjekt for elektronisk kommunikasjon ved tinglysing av 3.5.2007 nr. 0476.

[24] Sertifisering av ledelsessystem for informasjonssikkerhet – anerkjent standard for datasikkerhet.

- Elektronisk signering av tilbud i forbindelse med offentlige anskaffelser. Dette gjelder når det i eller i medhold av tinglysingsloven er krav om underskrifter på dokument, og det brukes elektronisk kommunikasjon.

4. Bruke standard for sikker datakommunikasjon fra offentlige nettsteder (HTTPS)

HTTPS er overføring av nett-trafikk over en sikker forbindelse. Ved å bruke krypteringsprotokollen Transport Layer Security (TLS) kan klienten verifisere identiteten til tjenesteleverandøren, og nett-trafikken kan overføres kryptert – som gjør det uleselig for uvedkommende under transporten.

Krav om sikker datakommunikasjon fra offentlige nettsteder kom i oktober 2021. I forskrift om IT-standarder i offentlig sektor, § 11. Obligatoriske standarder for kryptert datakommunikasjon med offentlige nettsteder og –tjenester, står det:

«Nettsteder og andre offentlige tjenester, herunder applikasjonsgrensesnitt (API-er), som benytter hypertekstoverføringsprotokollen (http) skal kryptere kommunikasjonen med transportlagssikkerhet i henhold til standarden HTTP over TLS [RFC 2818] ved bruk av protokollene HTTP/1.1 [RFC 7230 til RFC 7235] og TLS 1.2 [RFC 5246] eller TLS 1.3 [RFC 8446]. Fram til 1.1.2024 skal TLS 1.2 brukes, hvis en av kommunikasjonspartene ber om det. Kravet gjelder ikke lukkede tjenester hvor forvaltningsorganet ivaretar sikkerheten på annen måte. Dersom en tjeneste får en forespørsel om kommunikasjon over HTTP uten bruk av TLS skal tjenesten svare ved omdirigering til samme URL med bruk av HTTP over TLS».

Utover de fire **skal-kravene**, har Digdir også definert **syv anbefalte** løsninger for kommunens informasjonssikkerhet. Kommunen bør bruke:

1. grunnprinsippene for IKT-sikkerhet
2. rettleder om internkontroll i praksis (utredet sammen med skal-kravet til internkontroll)
3. standard for filoverføring
4. standard for sikker bruk av domenenavn
5. standarder for sikring av kommunikasjonskanaler
6. standarder for å motvirke falske avsendere av e-post
7. standarder for sikring av e-post.

Nasjonal sikkerhetsmyndighet (NSM) sin veileder **«Grunnprinsipper for IKT-sikkerhet»** beskriver hva en virksomhet bør gjøre for å sikre et IKT-system, og hvorfor. Grunnprinsippene er et supplement til eksisterende nasjonale og internasjonale regelverk, standarder og rammeverk innen IKT-sikkerhet, og uthever de viktigste sikringstiltakene i ISO/IEC 27002.
NSM påpeker at hvilke anbefalinger som er relevante vil variere med type virksomhet, og for store virksomheter vil de fleste tiltakene være relevante. Veilederen oppdateres jevnlig basert på innspill fra brukere og fagmiljøer fra offentlig og privat sektor.

Ifølge veilederen vil en angriper som regel bruke enkleste veien inn i systemene. Om det finnes sikringstiltak som er enkle å omgå vil angriperen lete etter, og utnytte, dette. Sårbarheter kan oppstå dersom kvaliteten på anskaffelsesprosessen ikke er god nok slik at komponenter eller tjenester med manglende sikkerhetsfunksjonalitet, manglende sikkerhetsrettinger eller feil konfigurasjon innføres. Sårbarheter kan også skyldes feil på produktet, plantede sårbarheter, oppdateringer eller vedlikehold. For i størst mulig grad å hindre sårbarheter fra å oppstå bør sikkerhet være en del av virksomhetens tankegang fra beslutning og anskaffelse til drift, vedlikehold og avskaffelse.

Veilederen er delt i **fire kategorier**, med til sammen 21 prinsipper, som hver beskriver tiltak som virksomheten bør implementere for å sikre sine systemer:

1. **Identifisere og kartlegge –** opparbeide og forvalte forståelse om virksomheten herunder leveranser, tjenester, systemer og brukere.

Manglende styringsstrukturer og prosesser for risikovurdering kan føre til at ledelsen ikke får tilstrekkelig informasjon til å prioritere og styre virksomhetens sikkerhetsarbeid.
Prinsippet med å **kartlegge** styringsstrukturer, leveranser og understøttende systemer, handler om at virksomheten må **identifisere**, prioritere og beskytte sine viktigste leveranser. Mangelfull oversikt kan føre til at enkelte, mindre viktige deler av IKT-systemet kan være godt sikret, mens andre mer vesentlige deler er eksponert og sårbart for angrep.

Kartlegging av enheter og programvare er viktig for å få oversikt over hva som befinner seg i virksomheten. En slik kartlegging bør avdekke både virksomhetsstyrte enheter, legitime enheter med begrensede rettigheter (for eksempel IoT[25]-enheter) og ukjente enheter (eks. ansattes private utstyr eller ondsinnede enheter). Kartleggingen bør dekke all programvare som brukes i virksomheten, både installert av IT-avdelingen og uautorisert programvare. Virksomheten bør få oversikt over enheter, programvarer og sårbarheter før eventuelle angripere gjør det.

En angriper har ofte som mål å øke sin tilgang, ofte gjennom å ta over ulike kontoer og søke seg til større rettigheter. Ved å **kartlegge** brukere og behov for tilgang minimeres risikoen for at brukere har tilgang til systemer og tjenester de ikke har behov for, og med mer rettigheter enn nødvendig for å gjøre jobben sin. NSM anbefaler at tilgangene til de ulike delene av et informasjonssystem deles opp, for å redusere skaden ved kompromittering eller utro ansatte.

2. **Beskytte og opprettholde –** prinsipper som må til for å ivareta en sikker tilstand for IKT-miljøet for å motstå eller begrense skaden fra dataangrep.

Ved å ivareta sikkerhet i anskaffelses- og utviklingsprosesser vil virksomheten minimere risikoen for at nye IKT-produkter og IKT-tjenester innfører konfigurasjonsmessige og arkiteturmessige sårbarheter. Sikkerhet er ikke kun viktig ved anskaffelse av rene sikkerhetsprodukter som eks. en brannmur. Om virksomheten anskaffer IKT-produkter og –tjenester med svak sikkerhet eller dårlig integrasjon med øvrig sikkerhetsarkitektur og produkter, kan det øke sårbarheten og redusere sikkerhetsnivået i IKT-systemet. Hvis virksomheten mangler gode prosesser for utvikling, test, verifisering og implementering vil sannsynligheten være stor for at sårbarhetene ikke blir oppdaget.

Etablere en sikker **IKT-arkitektur.** Angripere går minste motstands vei, slik at dårlig planlegging, mangelfull kontroll ved byggeprosess og/eller manglende vedlikehold kan det føre til mange hull og inngangsdører som en angriper kan benytte seg av. For god sikring beskrives viktige momenter som å sikre at alle virksomhetens IKT-produkter fungerer godt og sikkert sammen, drift og sikkerhetskonfigurasjon bør skje sentralt og likt per type enhet, samt at IKT-systemet bør deles opp i forskjellige deler etter tillitsnivå – for å begrense konsekvenser ved eventuelt angrep eller menneskelig feil.

De fleste IKT-produkter leveres med en standardkonfigurasjon fra produsent eller forhandler, som vanligvis er utviklet for å forenkle installasjon eller bruk. Åpne tjenester og porter, standardkontoer og passord, eldre protokoller og forhåndsinstallert programvare kan gi angripere en rekke muligheter til å få uautorisert tilgang. Virksomheten bør ivareta en **sikker konfigurasjon** av sine maskin- og programvarer, og herde sine produkter, slik at det tilfredsstiller sikkerhetsbehovet. Det bør være etablert rutiner for sporing, rapportering og korrigering av sikkerhetskonfigurasjon på enheter, programvare og tjenester.

[25] Internet of Things – samlebegrep for enheter som kan kobles til internett, eks. klokker, avtrekksvifter, biler mv.

Virksomhetens eget nettverk kan være spredt over flere geografiske lokasjoner, og tjenester kan også være satt ut til leverandører. Tilkobling av virksomhetens nettverk til internett eller andre nettverk utenfor virksomhetens kontroll eksponerer systemene for nye angrepsflater. I tillegg kan enheter og datatrafikk angripes fra innsiden; kompromittert server eller klient, utro tjener, kompromitterte leverandører med tilgang til nettverket, svakt sikret trådløse nett eller manglende fysisk sikring av porter/kabler. Det er derfor viktig å beskytte virksomhetens **nettverk** godt mot interne og eksterne trusler, og tilgangen til nettverket bør sikres og dataflyt på nettverket bør beskyttes med kryptering.

Det bør være kontroll på **dataflyt**, både mellom de ulike delene av egne systemer, og inn og ut av virksomheten. Det er viktig for, blant annet, å hindre at kompromittering av en enhet eller sone sprer seg videre i nettverket, for å tvinge datatrafikk gjennom virksomhetens sikkerhetstiltak, og for å isolere enheter som er spesielt kritiske sårbare eller eksponerte.

Prinsippet om å ha **kontroll på identiteter og tilganger** er nært knyttet mot kartlegging av brukere og tilganger, under kategorien identifisere og kartlegge. Ansatte med flere rettigheter enn de trenger ser et problem for mange, blant annet er det vanlig at alle ansatte kan skrive til og slette alt av filer og filmapper, og kan kjøre alt som finnes av programvare. Dette er kanskje ikke nødvendig for gjennomføring av jobben, men kan være til stor hjelp for en som ønsker å angripe virksomheten. Hvis alle har rettigheter til alt, vil kompromittering av én bruker kunne kompromittere hele IKT-systemet. For å redusere skaden bør rettigheter til ulike deler av informasjonssystemet deles opp, og en virksomhet må ha kontroll på brukerne – altså kontoer, rettigheter og tilganger de disponerer.

Kryptering er en forutsetning for beskyttelse av IKT-systemet. I en virksomhet er det ulike typer informasjon med ulikt behov for beskyttelse, og virksomheten må beskytte data **i ro og i transitt.** Dersom virksomhetsdata ikke krypteres kan uvedkommende lese eller manipulere den, og føre til at informasjonens konfidensialitet og integritet brytes. Samme risiko er til stede om programvaren eller maskinvaren som brukes er implementert med utilsiktede sårbarheter, eller om krypteringsnøkler er svakt beskyttet.

For å minimere angriperes mulighet til å manipulere menneskelig oppførsel i forbindelse med bruk av epostklienter og nettlesere bør virksomheten **beskytte e-post og nettleser.** Funksjoner og applikasjoner som skal motta og behandle data fra ukjente eksterne filer er ekstra utsatt for angrep. E-post og nettsider med skadevare (virus, trojanere, osv.) er vanlige inngangsportaler for angrep. Vedlegg og lenker i e-post er en av de vanligste inngangsveiene for distribuering av datavirus, ormer og annen type skadevare. Slike vedlegg og lenker utnytter ofte sårbarheter i andre applikasjoner, eller filtypen som vises i epostklienten (.JPG, .exe, .ZIP, osv.) kan være feil i forhold til faktisk filtype.

Virksomheten bør etablere evne til **gjenoppretting av data**. Enkelte dataangrep kan føre til at kritiske konfigurasjoner, programvare eller informasjon endres eller gjøres utilgjengelig, noe som kan påvirke virksomhetskritiske prosesser. Eksempelvis ble Østre Toten kommune utsatt for kryptovirus/løsepengevirus i 2021, noe som blant annet førte til lekking av personsensitiv data og utestengelse fra egen systemer i flere uker. I dette tilfellet førte også den manglende informasjonssikkerheten til at Datatilsynet valgte å bøtelegge kommunen.

For å opprettholde virksomhetens etablerte sikkerhetstilstand ved planlagte endringer er det viktig at virksomheten **integrerer sikkerhet i prosess for endringshåndtering.** Det vil alltid være behov for endringer i en virksomhet, blant annet som følge av oppgradering og utskifting av IKT-utstyr, og organisatorisk vekst eller tilpasninger, sammenslåing av virksomheter eller tjenesteutsetting. Alle endringer som gjøres kan påvirke virksomhetens etablerte sikkerhetstilstand, og det er viktig at virksomheten forstår konsekvensen av endringene, og justerer og konfigurerer IKT-systemene for å tilpasse seg disse.

Her bør det også gjennomføres tilstrekkelig med testing for å verifisere at ønsket sikkerhetstilstand opprettholdes.

3. **Oppdage –** prinsipper som ivaretar behovet for å håndtere endringer, både planlagte endringer, feilretting og sikkerhetsoppdateringer for å opprettholde den sikre tilstanden over tid.

Selv de beste produkter har feil og sårbarheter i seg, som kan utnyttes av angripere. Ondsinnet programvare kommer seg inn gjennom blant annet sluttbrukerutstyr, e-postvedlegg, nettsider, skytjenester og flyttbare medier. Virksomheten bør ha rutiner for å **oppdage og fjerne** kjente sårbarheter og trusler.

Ved å etablere **sikkerhetsovervåkning** av sine IKT-systemer og samle inn relevante data for å oppdage sikkerhetshendelser, kan virksomheten legge et grunnlag for analyse av data. Dette kan bidra til å oppdage sikkerhetshendelser tidlig, vurdere skadeomfang og hendelsens karakter, og forstå hendelsesforløpet. Mangelfull sikkerhetsovervåkning og deteksjon i informasjonssystemer, og mangelfull sammenstilling og analyse av sikkerhetsrelevante data hjelper angripere med å skjule tilstedeværelse, handlinger og aktiviteter i virksomhetens systemer.

Analyser data fra sikkerhetsovervåkning. Det kan være utfordrende å oppdage uautoriserte handlinger og sikkerhetstruende hendelser. Sammenstilling og analyse av innhentet data bidrar til å øke sjansen for å avdekke hendelser. Virksomheten bør være i stand til å finne kjente trusler i egen infrastruktur, ha kompetanse til å benytte automatiserte verktøy, og forstå hvordan disse kan utnyttes best mulig.

Virksomheten bør teste elementer i egne forsvarsmekanismer ved å gjennomføre **inntrengningstester**. Slike tester bør gjøres jevnlig for å verifisere etablerte sikkerhetstiltak, identifisere mangler og vurdere egen beredskap. Eksempler på svakheter kan være for langt tidsvindu fra annonsering av sårbarhet og sikkerhetsretting fra leverandør til installasjon i virksomheten, vide brukertilganger i kombinasjon med svake autentiseringsløsninger, mangelfull etablering av sikker konfigurasjon av enheter, manglende evne til å forstå egne verdikjeder og avhengigheter mellom systemer.

4. **Håndtere og gjenopprette –** prinsipper for å få på plass aktiviteter for å håndtere oppdagede sikkerhetstruende hendelser.

Forbered virksomheten på **håndtering** av hendelser slik at hendelser oppdages hurtig, kontrolleres, skaden minimeres og hendelsesårsaken fjernes effektivt. Dette inkluderer gjenopprettelse av integriteten til systemer og nettverk. Når hendelsen inntreffer er det for sent å utarbeide gode prosedyrer, rapporteringsrutiner, datainnsamling, ledelsesansvar og kommunikasjonsstrategier. Slike ting må være på plass og øves jevnlig for å gjøre virksomheten i stand til å forstå, håndtere og gjenopprette normaltilstand.

Vurdering og klassifisering av hendelser er viktig for at virksomheten kan disponere ressurser fornuftig og løse hendelsen så raskt som nødvendig. Feilaktig klassifisering kan føre til at en virksomhet bruker mye tid og krefter på uvesentlige hendelser mens viktigere hendelser går under radaren.

Det er viktig å kontrollere og håndtere hendelser slik at de håndteres riktig og med riktige ressurser, for å minimere spredning og konsekvenser, og normaltilstand opprettholdes/gjenopprettes effektivt. I etterkant er det viktig å **evaluere og lære** av hendelser. Dette gjør virksomheten i stand til å forbedre sikkerhetstiltak, hendelsesprosesser, opplæring av personell og oppdatering av gjeldende prosedyrer.

Etter Digdirs anbefaling bør offentlige kommunikasjonstjenester støtte FTP (File Transfer Protocol) som protokoll for filoverføring. Protokollen har begrenset sikkerhet, og bør brukes over en sikker kommunikasjonskanal.

Kommunen bør også bruke **standard for sikker bruk av domenenavn**, som har som formål å redusere risikoen for brudd på integritet ved oppslag i domenenavnsystemet. Mer konkret er DNSSEC (DNS[26] Security Extensions) en sikkerhetsmekanisme som legges inn i domenenavnsystemet. Da vil svarene på et domeneoppslag signeres på en måte som gjør at det er mulig å kontrollere at de kommer fra riktig kilde og ikke er endret underveis. DNSSEC sikrer at du kommer til den adressen du vil nå, men ikke at innholdet på siden er trygt.

Det bør brukes standarder for **sikring av kommunikasjonskanaler.** VPN protokoller (Virtual Private Network) brukes for å sette opp sikre kommunikasjonskanaler mellom to eller flere endepunkt som kommuniserer over åpne nett. Det brukes kryptering og andre sikkerhetsmekanismer for å sikre at det kun er de autoriserte endepunktene som får tilgang til data som oversendes i kanalen.

DMARC[27] er anbefalt **standard for å motvirke falske avsendere av e-post.** Det fremkommer av Digdirs veiledning på området at DMARC anbefales brukt sammen med minst en av de underliggende standardene Sender Policy Framework (SPF) og Domain Keys Identified Mail (DKIM).

Standarder for sikring av e-post. Transportsikringen bruker kryptert kommunikasjon for å overføre meldinger mellom epostservere. Digdir viser her til NSMs veileder for grunnleggende tiltak for sikring av e-post. For overføring av e-post anbefales StartTLS[28], som er en beskyttelsesmekanisme som sørger for autentisering av eposttjenere og konfidensialitetssikring, og SPF som brukes for å spesifisere hvilke eposttjenere som er autorisert til å sende e-post på vegne av et gitt domene. For ytterligere sikring av e-post anbefaler NSMs veileder også DKIM og DMARC, som omtalt i forrige avsnitt.

På bakgrunn av dette har revisjonen formulert følgende revisjonskriterier:

Kommunen skal:
Kommunen skal ha etablert en tilstrekkelig god internkontroll på informasjonssikkerhetsområdet.
Internkontrollsystemet skal være basert på en vurdering/identifisering av relevante lov- og regelverk og skal omhandle følgende punkter gjeldende for kommunens IKT-sikkerhet:

- Kommunen har planer og rutiner (sikkerhetstiltak) for å sikre beredskap ved sikkerhetshendelser.
- Kommunen gjennomfører risikovurderinger knyttet til IKT-sikkerhet.
- Det er utarbeidet rutiner for å varsle om IKT-sikkerhetshendelser. Herunder om det skal varsles til de sektorvise responsmiljøene (SRM) og eventuelt samarbeidende virksomheter, samt til NSM om nødvendig.
- Kommunen vurderer behov for bistand ved IKT-sikkerhetshendelser.
- Kommunen skal bruke kravspesifikasjon for PKI ved anskaffelse av PKI-tjenester, når det er obligatorisk.
- Kommunen skal bruke IPv4 og IPv6 ved kommunikasjon på internett, og vurdere om nytt IT-utstyr støtter disse protokollene.
- Kommunen skal bruke HTTPS på sine nettsteder, og ved eventuelle andre offentlige tjenester der http-protokoll brukes for overføring.

[26] Domain Name Server – oversetter nettadressen du skriver inn i adressefeltet til en IP-adresse.

[27] Domain-based Message Authentication, Reporting, and Conformance. Se mer om DMARC hos NSM.

[28] En beskyttelsesmekanisme for overføring av e-post mellom e-posttjenere, se NSM.

Kommunen bør:

- Kommunen bør bruke NSM sine grunnprinsipper for IKT-sikkerhet i sitt arbeid med informasjonssikkerhet, herunder bør de;
    - identifisere, prioritere og beskytte sine viktigste leveranser
    - kartlegge hva de har av enheter og programvare, samt brukere og behov for tilganger
    - dele opp IKT-systemet i ulike deler etter tillitsnivå, og utføre drifts- og sikkerhetskonfigurasjoner sentralt og likt for hver type enhet
    - ivareta en sikker konfigurasjon av sine maskin- og programvarer, og herde sine produkter, slik at det tilfredsstiller sikkerhetsbehovet
    - ha etablert rutiner for sporing, rapportering og korrigering av sikkerhetskonfigurasjon på enheter, programvare og tjenester
    - sikre tilgangen til nettverk, og beskytte dataflyt på nettverket med kryptering
    - beskytte e-post og nettleser
    - etablere evne til gjenoppretting av data
    - integrere sikkerhet i prosess for endringshåndtering
    - ha rutiner for å oppdage og fjerne kjente sårbarheter og trusler
    - være i stand til å finne kjente trusler i egen infrastruktur, ha kompetanse til å bruke automatiserte verktøy, og forstå hvordan disse kan utnyttes best mulig
    - teste elementer i egne forsvarsmekanismer ved å gjennomføre inntrengningstester
    - forberede seg på håndtering av hendelser slik at de an oppdages hurtig, kontrolleres, skaden minimeres og hendelsesårsaken fjernes effektivt
    - vurdere og klassifisere, kontrollere og håndtere, og evaluere og lære av hendelser
- Kommunen bør bruke Digdirs «Interkontroll i praksis – informasjonssikkerhet» i arbeidet med internkontroll, konkretisert i følgende syv hovedpunkter:
    - Ledelsens styring og oppfølging
    - Vurdering av risiko
    - Håndtering av risiko
    - Overvåking og hendelseshåndtering
    - Måling, evaluering og revisjon
    - Kompetanse- og kulturutvikling
    - Kommunikasjon
- Kommunen bør bruke DNSSEC for å redusere risikoen for brudd på integritet ved oppslag i domenenavnsystemet.
- Kommunen bør bruke DMARC for å motvirke falske avsendere av e-post. DMARC brukes som anbefalt sammen med SPF og/eller DKIM.
- Kommunen bør bruke STARTTLS og SPF for transportsikring av e-post.
- Kommunen bør støtte FTP som protokoll for filoverføring.
- Kommunen bør bruke standarder fra Digdirs veiledning for bruk av VPN, for å sikre sine kommunikasjonskanaler.

Problemstilling 2
Har kommunens ansatte kjennskap til rutiner for IKT-sikkerhet?

Datatilsynet skriver følgende om brukeropplæring i sin veileder om internkontroll og informasjonssikkerhet: *«Målet med brukeropplæring er å sørge for at brukerne er oppmerksomme på trusler mot personvernet og informasjonssikkerheten generelt, og at de er gitt mulighet til å etterleve dette i sitt daglige arbeid. Opplæring bør være tilpasset ulike målgruppers behov for opplæring og fordeles over tid. Brukerne bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle risikoer.»* I henhold til veilederen, bør de ansatte ha fått hensiktsmessig opplæring før de får tilgang til informasjon eller tjenester. Dette inkluderer for eksempel at de kjenner til innloggingsprosedyrer, bruk av programvare, sikkerhetsinstruks og rapportering av avvik. I tillegg bør de ansatte, ifølge veilederen, få regelmessig oppdatering i organisasjonens policy og rutiner.

NSM viser til sikkerhetsloven med forskrifter i sin Veileder i personellsikkerhet, hvor bestemmelser knyttet til taushetserklæring og kompetanse fremgår.

På bakgrunn av dette har revisjonen formulert følgende revisjonskriterier:

- De ansatte har fått opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av IKT-systemer.
- De ansatte skal kjenne til kommunens egne rutiner og prosedyrer for IKT-sikkerhet.
- Det gjennomføres kompetansetiltak for medarbeiderne for å styrke IKT-sikkerheten.
- De ansatte har undertegnet en taushetserklæring ved inngåelse av arbeidsforholdet.