

VEDLEGG 2 GRUNNPRINSIPPER FOR SIKKERHETSSTYRING

Identifisere og kartlegge:

Danner grunnlaget for de andre kategoriene, vurdering av risiko og plan for risikohåndtering. Det er viktig med grundige analyser og vurdering av risiko, slik at tiltakene treffer og blir effektive.

Beskytte og opprettholde:

Tilpass virksomhetens sikkerhetsorganisasjon og styringssystem i forhold til risikovurderingene. Innfør sikkerhetstiltak for å oppnå et akseptabelt sikkerhetsnivå.

Oppdage:

Kontroller sikkerhetstilstanden for å oppdage eller avdekkes sårbarheter eller andre sikkerhetstruende forhold.

Håndtere og gjenopprette:

Skal gjøre virksomheten rustet til å gjennomføre tiltak for å redusere skadeomfanget og gjøre tiltak som gjenoppretter et akseptabelt sikkerhetsnivå i virksomheten.



Kommunens sakssystem for byggesaksbehandling blir utsatt for et løsepengevirus og data låses ned.

Kommunen settes ut av stand til å overholde lovpålagte frister for byggesaksbehandling. For involverte parter kan konsekvensene være økte kostnader, tap av inntekter og usikkerhet knyttet til fremdrift.

Risiko endrer seg over tid, blant annet i takt med:

- Verdier og teknologisk utvikling
- Endringer i lover, regler og rutiner
- Organisatoriske og prosessmessige endringer
- Globale, regionale og nasjonale trender
- Endringer i samfunnet
- Situasjonsavhengighet
- Hendelser

En uønsket hendelse vil få større konsekvenser dersom informasjon av høy verdi er involvert – det vil si at det er en høyere iboende risiko knyttet til behandling av en bestemt type informasjon. For eksempel vil det få større konsekvenser om det er innbyggernes helseopplysninger som berøres, enn om det er telefonnummer som enkelt kan finnes på et nettsted. Det vil derfor være større behov for å ivareta informasjonssikkerhet og personvern knyttet til helseopplysninger, og sikkerhetstiltakene vil derfor gjerne være flere eller strengere.

Kommunen bør ha oppdatert innsikt i overordnede trender og utviklingen i kommunens risikobilde. Fagpersoner på informasjonssikkerhets- og personvernområdet bør ha som oppgave å ivareta denne type risikovurderinger.

Kommunedirektøren **anbefales** å ha fokus på:

- Risikoene som berører særskilte kategorier personopplysninger eller særlig sårbare personer. For eksempel:
 - Helse- og omsorgstjenester for eldre
 - Helsestasjon for ungdom
 - Barnevernet
 - Tannhelse
 - Skole og barnehager
- Informasjon, personopplysninger eller IKT-systemer med høyest verdi for drift og tjenesteproduksjon. For eksempel:
 - Informasjon om vannforsyning og avløp
 - Informasjon om veier og broer
 - Risikovurderinger
 - Beredskapsplaner
- De sikkerhets- eller personvernmessige hendelser som kan medføre konsekvenser som at drift og tjenesteproduksjon ikke lar seg gjennomføre, eller med sterkt redusert kvalitet, dvs. de høyeste risikoene.
 - Nedetid for IKT-systemer som er kritiske for tjenesteproduksjon, for eksempel pasientjournal, saksbehandlingssystem for barnevern eller læringsplattformer.

Uønskede hendelser kan påvirke hvordan krav til tilgjengelighet, integritet og konfidensialitet er ivaretatt. I tillegg kan uønskede hendelser berøre personopplysninger og ha betydning for innbyggers eller ansattes rett til personvern. **Noen eksempler på uønskede hendelser:**

Scenarier

Alle IT-tjenester i helse og omsorg stopper opp i kommunen som følge av en brann som ødelegger datasenteret hvor kommunens servere driftes fra. Det tar 14 dager å sette opp et nytt datasenter. Rom må gjøres klar, utstyr kjøpes inn og IKT-systemene må konfigureres. Da backup skal hentes frem, viser det seg at data fra de siste 14 dager før brannen har gått tapt fordi backupene har vært oppbevart i samme bygg som datasenteret før de har blitt sendt til sikker oppbevaring. Det fører til at kommunen ikke har fullstendige pasientopplysninger og en pasient blir alvorlig syk fordi informasjon om endringer i helsetilstanden har gått tapt.

Det gjennomføres et hackerangrep mot skolene som fører til at personopplysninger om enkelte elever spres. En undersøkelse viser at sikkerhetskravene til pålogging har vært svake, og at en elev har klart å logge seg inn på en bruker med administratortilganger og herfra delt personopplysninger. Saken får stor medieomtale, og kommunens omdømme svekkes.

En av kommunens innbyggere har en mor som er beboer på et av kommunens pleiesentre. Innbyggeren er verge for moren. I en samtale med en kommunalt ansatt, som også jobber i helse- og omsorgstjenesten, men i en annen avdeling, får innbyggeren en følelse av at vedkommende har innsikt i morens pleieforhold. Som følge av dette ber innbyggeren om at det undersøkes hvem som har vært inne og sett på morens journalopplysninger. Loggen viser at en person som ikke har tjenstlig behov har sett på morens opplysninger i journalsystemet. Det iverksettes en intern undersøkelse. Den det gjelder innrømmer å ha snoket i pasientjournaler, med den følge at den det gjelder avskjediges.

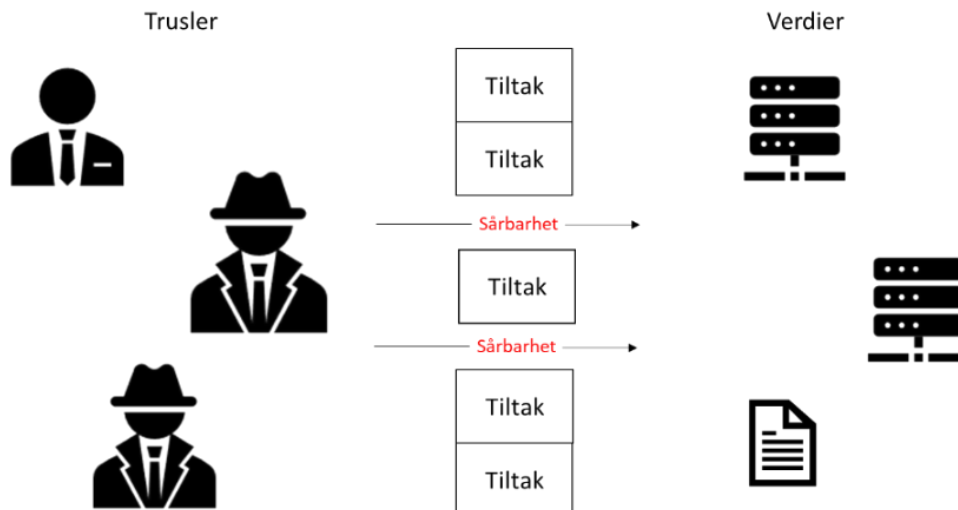
Kommunens regnskapssjef får en e-post fra driftsleverandøren av økonomisystemet med melding om at det er problemer med hans konto i systemet. Brukernavn og passord er utløpt. Ettersom regnskapssjefen nettopp er tilbake fra ferie tenker hun ikke mer på det, og går inn på nettskjemaet hun har fått en lenke til. Hun fyller ut skjemaet og trykker ok. Da hun får svar, og forsøker å logge inn igjen i økonomisystemet, kommer hun ikke inn igjen. Etter kort tid opplever alle ansatte det samme: ingen kommer inn i noen av kommunens systemer. Kommunen har blitt utsatt for et løsepengevirus, og løsepenger må betales ut for å få tilgang til kommunens IT-systemer igjen.

Kommunen anskaffer et nytt HR-system. Som en del av anskaffelsen gjennomføres det sikkerhetstester og funksjonstester i leverandørens sikkerhetsmiljø. For å få gode tester benyttes data hentet fra HR-systemet som er i drift. Leverandøren har en underleverandør i et annet land som gjennomfører sikkerhetstesting. Media plukker opp saken og skriver om den. Når Datatilsynet fatter interesse for saken får kommunen bøter på grunn av bruken av ansattes personopplysninger i strid med behandlingsgrunnlaget og overføringen av data til dette landet. Foruten økonomiske konsekvenser som følge av boten får saken konsekvenser for de ansattes tillit til kommunen som arbeidsgiver. Flere ansatte velger derfor å slutte.

En kommunalt ansatt som er motstander av norske vaksinerådet endrer informasjon om COVID-vaksiner på kommunens hjemmesider i tråd med sitt politiske syn. I etterkant stilles det kritiske spørsmål til kommunens regime for tilgangsstyring og kontroll på endringer i ikt-systemer.

En underleverandør av kommunens pasientjournal-system (EPJ) har vært igjennom en omorganiserings- og nedbemanningsprosess med høyt konfliktnivå. En misfornøyd ansatt hos denne leverandøren kopierer ut all data fra kommunens EPJ, endrer data i EPJ og truer med å offentliggjøre dataene om hun ikke får utbetalt ti millioner kroner.

Behandling av personopplysninger med høy risiko for den registrerte, for eksempel behandling av helseopplysninger i store mengder, skal være gjenstand for en egen risikovurdering; en personvernkonsekvensvurdering. Vurdering



Figur 1: Kommunen har verdier som de ønsker å beskytte. For å gjøre dette iverksettes tiltak for å sikre verdiene. På venstre side i figuren finnes ulike trusselaktører som ønsker tilgang til verdiene. Dette kan være ansatte, fremmede stater eller andre som ønsker tilgang til informasjonen. Disse vil forsøke å utnytte sårbarheter hos kommunen. Dersom kommunen ikke adresserer sårbarhetene med relevante tiltak, vil det være lettere for trusselaktørene å få tilgang til verdiene.

og oppfølging av risiko knyttet til informasjonssikkerhet og personvern bør følge kommunens etablerte [rammeverk for risikostyring](#).

Uønskede hendelser har to komponenter som medfører at ting kan gå galt. Det ene er trusler kommunen står overfor, det andre er sårbarhetene kommunen selv har. Truslene kan være eksterne, for eksempel hackere, eller interne, for eksempel misfornøyde ansatte.



Kommunen feilkoder en bekymringsmelding til barnevernet med den følge at brev som burde vært unntatt offentlighet ligger åpent i offentlig postjournal. For kommunen medfører dette bot fra Datatilsynet og omdømmetap. Det alvorligste ved hendelsen er at bruddet i personvernet medfører svært negative konsekvenser for barnet og familien

Hvilke sikkerhetstiltak som mest effektivt kan bidra til å redusere høy risiko til et akseptabelt nivå kan være vanskelig å få et godt overblikk over. Det anbefales derfor å bygge et rammeverk som stiller krav til sikkerhetstiltak, og som bidrar til at kommunen forholdsvis enkelt kan få en god informasjonssikkerhet og godt personvern som bidrar til å håndtere mange risikoer. Nasjonal sikkerhetsmyndighet har etablert rammeverket «[Grunnprinsipper for IKT-sikkerhet](#)», som anbefales for blant annet offentlige virksomheter og virksomheter med kritiske samfunnsfunksjoner, slik som kommunen.

Ulike typer av informasjon med særlig høy verdi kan ha like sikkerhetsbehov, og informasjonssikkerhet og personvern kan i stor grad ivaretas gjennom de samme sikkerhetstiltakene. Gjennom en oversikt over verdiene kan informasjon grupperes slik at fokus og arbeid med sikkerhetstiltak særlig rettes mot informasjon, personopplysninger og IKT-systemer med høyest verdi. Eksempelvis kan sikkerhetstiltak for særskilte kategorier personopplysninger også benyttes for informasjonsverdier knyttet til samfunnskritiske oppgaver.

Kommunen kan for eksempel dele sine informasjonsverdier i fire grupper, og liste ulike tiltak og frekvens som vist i tabellen under. Figuren sier også noe om at et sett sikkerhetstiltak kan gjelde for ulike informasjonsverdier – forutsatt at de har en samsvarende verdi for kommunens drift og tjenester.

Informasjonsverdi	Eksempel på informasjon	Grad av sikkerhetstiltak	Kontrollfrekvens
Kritisk verdi	Informasjon som er kritisk for kommunen i en krisesituasjon., f.eks.: - informasjon om, eller som understøtter, samfunnskritiske funksjoner (typisk vannverk, kraftforsyning og vei). - beredskapsplaner, sensitive personopplysninger (inkludert helseopplysninger) og kode 6/7-opplysninger.	Høy	Fire ganger årlig
Høy verdi	Informasjon som vil være ødeleggende for funksjoner og tjenester som er kritisk for kommunens daglige drift, f.eks.: - strategidokumenter, eksamens- og tentamenoppgaver før de er gitt, - tilbud og protokoller for pågående anskaffelsesprosesser informasjonssystem for lønnsutbetaling.	Høy	Halvårlig
Middels verdi	Virksomhetsintern informasjon eller informasjon som kan skade kommunens funksjoner og tjenester i daglig drift, f.eks.: - læringsplattformen for kommunikasjon mellom elev og skole. - informasjon som er unntatt offentligheten.	Middels	Årlig
Lav verdi	Åpen informasjon uten spesielle sikkerhetsbehov, f.eks.: informasjon som ligger åpent på hjemmesiden til kommunen, som for eksempel organisasjonskart	Lav	Ingen aktiv oppfølging av sikkerhetstiltak

Figur 2: Eksempler på gruppering av informasjon.