ROS-analyse av Digital postkasse til innbyggere

Direktoratet for forvaltning og IKT

Innhold

1 Innledning

Høsten 2012 og våren 2013 ble det gjennomført en ROS-analyse av Digital postkasse til innbyggere (heretter omtalt som ROS1). Dette ble gjort i forkant av kravspesifikasjon og utlysning av konkurranse om meldingsformidlertjenesten og digitale postkasser. ROS-arbeidet måtte dermed baseres på et løsningskonsept og en del forutsetninger. Dette var et bevisst valg og ga kvalifiserte vurderinger som grunnlag for sikkerhetskrav som ble tatt inn i anskaffelsesprosessen. Kontrakter ble inngått i mars 2014 og produksjonssetting av tjenesten er planlagt til 18. november 2014. ROS-rapporten fra 2013 (ROS1) er nå revidert med bakgrunn i at løsningskonseptet for Digital postkasse til innbyggere er fastsatt, leverandører valgt og kontrakter inngått.

Arbeidet med ROS1 var grunnlaget for en rekke krav og tiltak til meldingsformidleren og postkasseleverandørene, for at tjenesten skal være sikker. I tillegg var dette arbeidet med på å definere en rekke funksjonelle krav og teknologivalg som har betydning for den utformingen tjenesten har fått. Disse valgene (som for eksempel kvitteringer på meldinger og kryptering av meldingene frem til postkassen) har redusert mye av risikoen som ble identifisert i ROS1. I arbeidet med ROS2 er det tatt utgangspunkt i de risikoer som ble rangert som høye (røde) eller moderate (gule) risikoer i ROS1. Slik tjenesten nå er utformet er det ikke igjen noen risikoer vurdert som høye (røde). De risikoer fra ROS1 som er vurdert som moderate(gule) er tatt med i ROS2, og behandlet i denne rapporten. I tillegg er det vurdert om det foreligger nye risikoer. Prosjektgruppen som har gjennomført denne ROS-analysen er av den oppfatning at leverandørene som har kontrakter på levering av meldingsformidlertjenesten og digitale postkasser, har et bevisst forhold til sikkerhetsarbeid og sikker forvalting av den informasjonen som går igjennom tjenesten.

Prosjektet har fulgt standarden ISO/IEC 27005:2011 i arbeidet med å gjennomføre risikovurderingen, jf. Standardiseringsrådets anbefaling av 13. mars 2012. Termen *standarden* benyttes isteden for *ISO/IEC 27005:2011* nedenfor. Med Normen menes «*Norm for informasjonssikkerhet i helse-omsorgs- og sosialsektoren (2010)*[1]» og med *Faktaark* de faktaarkene som er utarbeidet i tråd med Normen. Under revisjonen av den tidligere ROS-analysen er metode og arbeidsform beholdt. Fokus har vært å oppdatere tidligere funn utfra inngåtte kontrakter og leverandørenes implementasjoner av tjenestene.

Selv om ROS-analysen gjennomføres i henhold til standarden ligger det utenfor mandatet å foreslå organisatoriske grep nødvendige for å få etablert en prosess for risikohåndtering som beskrevet i standardens del 7.4. Ansvaret for de organisatoriske grepene hos avsender ligger hos de ulike avsendervirksomhetene.

Den kontekst som ble etablert for ROS1 som identifiserte risikoer som verdier i systemet utsettes for, og presenterte forslag til tiltak for å redusere risiko, har vært utgangspunkt for arbeidet. Konteksten fra ROS1 er i store trekk gjenbrukt, da det ikke er vesentlige endringer på det overordnede konseptet for sikker digital postkasse. En viktig endring er imidlertid at sannsynlighetsskalaen er justert slik at

[1] http://normen.no

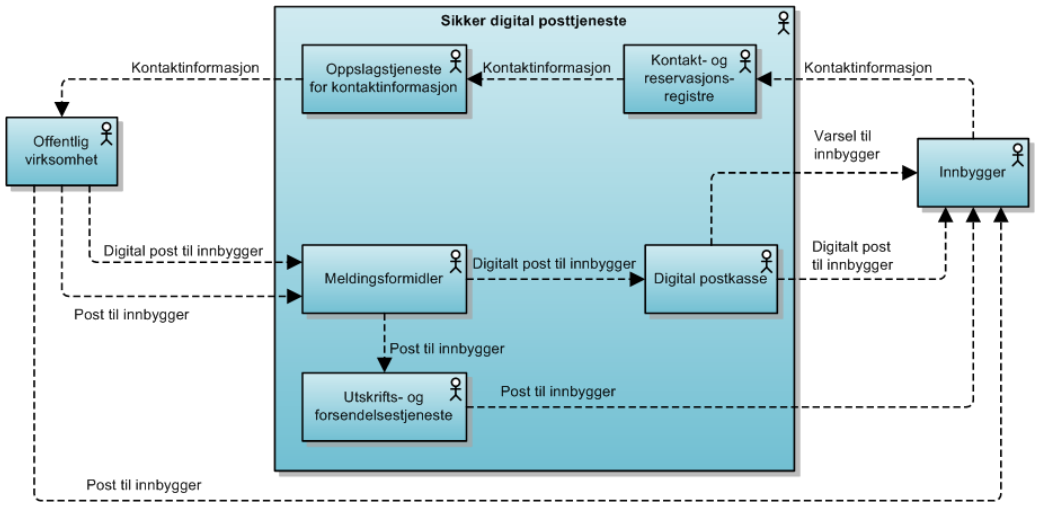
denne nå er mer realistisk. Skalaen er nå den samme som er benyttet i ROS-analysen av Kontakt- og reservasjonsregisteret, se punkt 3.5

Prosjektet har gjennom møter med de fire oppstartsvirksomhetene (de første virksomhetene som tar i bruk digital postkasse til innbygger – NAV, Statens innkrevingssentral, Kreftregisteret og KS SvarUT) innhentet informasjon og kunnskap om deres syn på risiko forbundet med å ta i bruk Digital postkasse til innbyggere (identifisering av risiko og analyse av disse). I tillegg er det benyttet en referansegruppe hvor alle virksomheter som deltar i styringsrådet for Difis felleskomponenter har vært inviterte til å delta i tillegg til de virksomhetene som deltok i ROS1[2].

1.1 Hva er Digital postkasse til innbygger?

Digital postkasse til innbyggere skal gjøre post fra det offentlige tilgjengelig for innbyggerne i en digital postkasse som innbygger selv har valgt hos en av de to markedsaktørene som har avtale med Difi (e-Boks og Digipost). De to kjernefunksjonene er at innbyggeren skal kunne motta og lagre post fra forvaltningen på en sikker måte, så lenge innbygger selv ønsker.

Denne rapporten redegjør for en oppdatert status for trusselbildet knyttet til Digital postkasse til innbyggere, og gir vurderinger av hvilke eventuelle ytterligere sikkerhetstiltak som bør iverksettes.



Figur 1 Overordnet konsept og informasjonsflyt for Digital postkasse til innbyggere

- *Oppslagstjeneste for kontaktinformasjon* gir offentlig forvaltning tilgang til opplysningene i kontakt- og reservasjonsregisteret. Dette er innbyggeres egenregistrerte kontaktinformasjon (e-postadresse og mobilnummer), reservasjonsstatus, valgt digital postkasse for mottak av digitale

[2] Følgende virksomheter har deltatt i referansegruppen: Skatteetaten, NAV, Brønnøysundregistrene, Lånekassen, Samordna opptak, KS/KommIT, Politidirektoratet, Statens Pensjonskasse, Helsedirektoratet, Bergen kommune

brev fra offentlig sektor, og sertifikatinformasjon som skal benyttes for kryptering til en digital postkasse eller utskriftsleverandøren.

- *Kontakt- og reservasjonsregisteret* inneholder kontaktinformasjon for mer enn 3,4 millioner innbyggere. Registeret inneholder informasjon om:
  - Hvorvidt innbyggere har reservert seg mot digital kommunikasjon mot det offentlige eller ikke, i henhold til eForvaltningsforskriften § 9.
  - Foretrukket e-postadresse og mobilnummer
    - Innbyggere kan kun registrere én e-postadresse og ett mobilnummer i registeret, og må ikke registrere begge deler.
  - Adresse til mottakers digital postkasse for mottak av digitale brev fra offentlig sektor
  - Sertifikatinformasjon for postkasseleverandører, som har avtale med Difi.
  - Sertifikatinformasjon for utskriftsleverandør (kommer når utskrifts- og forsendelsestjenesten produksjonssettes i Q1 2015).
- *Meldingsformidler* er offentlig virksomheters grensesnitt mot digital postkasse til innbygger og har ansvaret for å formidle post til innbygger som digitale brev til innbyggers selvvalgte digitale postkasse. Meldingsformidleren kan også benyttes for utskrift og forsendelse av papirbrev til innbyggers postadresse dersom virksomheten ønsker dette.
- *Digital postkasse*: Innbyggers selvvalgte digitale postkasse som har ansvaret for å gjøre tilgjengelig og oppbevare innbyggers digitale brev fra det offentlige.
- *Utskrifts- og forsendelsestjeneste:* Tjeneste tilknyttet meldingsformidleren for utskrift og forsendelse av papirbrev til innbyggers postadresse

1.1.1 Aktører

Følgende aktører er involvert i digital postkasse til innbyggere:

Aktør	Beskrivelse
Sentralforvalter	Difi er forvalter av digital postkasse til innbygger
Offentlig virksomhet	Virksomhet som sender meldinger gjennom løsningen til innbygger. Må akseptere Difis bruksvilkår før integrasjon. Kan være en offentlig virksomhet, eller virksomheter som opptrer på vegne av det offentlige. Benevnes som «virksomhet eller avsendervirksomhet» i dette dokumentet.
Innbygger	Privatperson som kan eller har opprettet digital postkasse for mottak av post fra det offentlige. Også omtalt som «person».
ID-porten	Felleskomponent for autentisering i offentlig sektor. Brukes for innlogging til postkassene når innbyggere ønsker tilgang til sin digitale post fra det offentlige.
Leverandør av meldingsformidler	Posten Norge AS ved Digipost er leverandør av meldingsformilderen
Leverandører av Digital postkasse	e-Boks A/S og Posten Norge AS ved Digipost er leverandører av digitale postkasser til innbyggere.

1.1.2 Kilder til data i Digital postkasse til innbyggere

Kilde	Beskrivelse
Innbygger	Innbygger selv inngår avtale med den postkasseleverandør han velger å benytte for mottak av post fra det offentlige og registrer sin kontaktinformasjon hos leverandøren og i kontakt- og reservasjonsregisteret.
Postkasseleverandør	Oppdaterer Kontakt og reservasjonsregisteret med korrekt postkasseadresse og sertifikat for kryptering av meldinger når innbygger velger leverandøren for mottak av post fra det offentlige. Mottar meldinger med tilhørende metadata fra meldingsformidleren og sender forskjellige kvitteringsmeldinger til denne.
Meldingsformidleren	Mottar meldingen og tilhørende metadata fra Avsendervirksomhetene og videreformidler disse til korrekt postkasseleverandør. Gjør egne og de digitale postkassenes kvitteringsmeldinger tilgjengelig for avsendervirksomhetene
Sentralforvalter	Visse endringer tilknyttet opprydding og verifikasjon gjennomføres av forvalter av kontakt- og reservasjonsregisteret, eksempelvis sletting av ugyldige identiteter. Sentralforvalter vil kunne sende testmeldinger når det er behov for dette.
Avsendervirksomhetene	Er kilder til meldinger og tilhørende metadata som formidles til innbygger gjennom digital postkasse til innbygger.

1.1.3 Sletting av brev i digital postkasse

Post som er lagt i den digitale postkassen er innbyggers eiendom. Dersom innbygger ønsker å slette hele eller deler av innholdet i postkassen, er det innbyggers valg. Det er implementert mekanismer som forhindrer at meldinger slettes på grunn av brukerfeil. I utgangspunktet kan ikke en melding trekkes tilbake når den er tilgjengeliggjort i innbygger postkasse.

Dersom mottaker dør vil, avdødes postkasse oppbevares i en periode etter at postkasseleverandøren mottok melding om dødsfallet. Arvingene får tilgang til avdødes postkasse ved fremvisning av skifteattest.

Sikkerhetskopier oppbevares i 6 uker eller to måneder avhengig av postkasseleverandør.

1.1.4 Overordnet teknisk beskrivelse

For teknisk systembeskrivelse henvises det til oppdatert dokumentasjon http://begrep.difi.no/SikkerDigitalPost/.

1.1.5 Taushetsbelagte opplysninger

Det er opp til avsender å avgjøre hvordan meldinger skal sendes, og avsenderne må velge en forsendelsesmåte (uavhengig av om den er på papir eller digital) som tilfredsstiller behovet for sikkerhet, funksjonalitet og brukervennlighet. Digital postkasse til innbyggere er konstruert for å kunne håndtere taushetsbelagte opplysninger og annen beskyttelsesverdig informasjon. Det er iverksatt strenge sikkerhetstiltak for å hindre misbruk av opplysningene som sendes til postkassen.

Kun et mindre antall personer hos postkasseleverandøren har autorisert tilgang til postkassen og minst to personer må være involvert for å få tilgang til meldingsinnholdet. Metadata om kommunikasjonen er tilgjengelig hos noe flere personer, samt hos meldingsformidler. Eventuell tilgang til slike opplysninger skal loggføres. Systemene er godt sikret mot uvedkommendes tilgang, og i postkassen er også meldingene lagret i kryptert form.

For noen taushetsbelagte opplysninger kan det være særlig høye beskyttelsesbehov. Spesielt antas dette å kunne gjelde sendinger til innbyggere med adressesperring i folkeregisteret (kode 6), jf. at hvis trusselutøveren klarer å lokalisere innbyggeren kan det innebære fare for liv eller helse. Avsendervirksomhetene er nærmest til å vurdere hvilken risiko forsendelse til kode 6-personer eventuelt innebærer, herunder om metadata (avsenders identitet) vil være geolokaliserende i det enkelte tilfellet. Avsender må vurdere hvilke tiltak som best møter risikobildet. Et mulig tiltak kan være å beskrive avsender på en ikke-geolokaliserende måte (eks. «din hjemkommune» i stedet for kommunens navn).

Difi har hatt dialog med politiet om hvordan personer som er beskyttet i henhold til kode-6 i folkeregisteret bør håndteres. Det anses som ønskelig at personer i kode-6 skal kunne være digitale, jf. at digital forsendelse kan gå vesentlig raskere enn papirpost med videresending. Det anbefales imidlertid at man i stor grad benytter opplysninger som ikke inneholder f.eks. geolokaliserbare data og andre sporbare data i metadata.

1.1.6 Graderte opplysninger

Tjenesten er ikke tilrettelagt for å behandle informasjon som er gradert etter sikkerhetsloven.

1.2 Metode og arbeidsform

Prosjektet har fulgt standarden ISO/IEC 27005:2011 i arbeidet med å gjennomføre ROS-analysen, jf. Standardiseringsrådets anbefaling av 13. mars 2012. Termen *standarden* benyttes isteden for *ISO/IEC 27005:2011* nedenfor. Med Normen menes «*Norm for informasjonssikkerhet i helse- omsorgs- og sosialsektoren*» (2013) og med *Faktaark* de faktaarkene som er utarbeidet i tråd med Normen. Normen med veileder for risikovurdering og faktaarkene er i denne ROS-analysen benyttet til innspill, til definisjon av sannsynlighetsnivåer og konsekvens. Det er også Datatilsynets veileder for risikovurdering i informasjonssystemer.

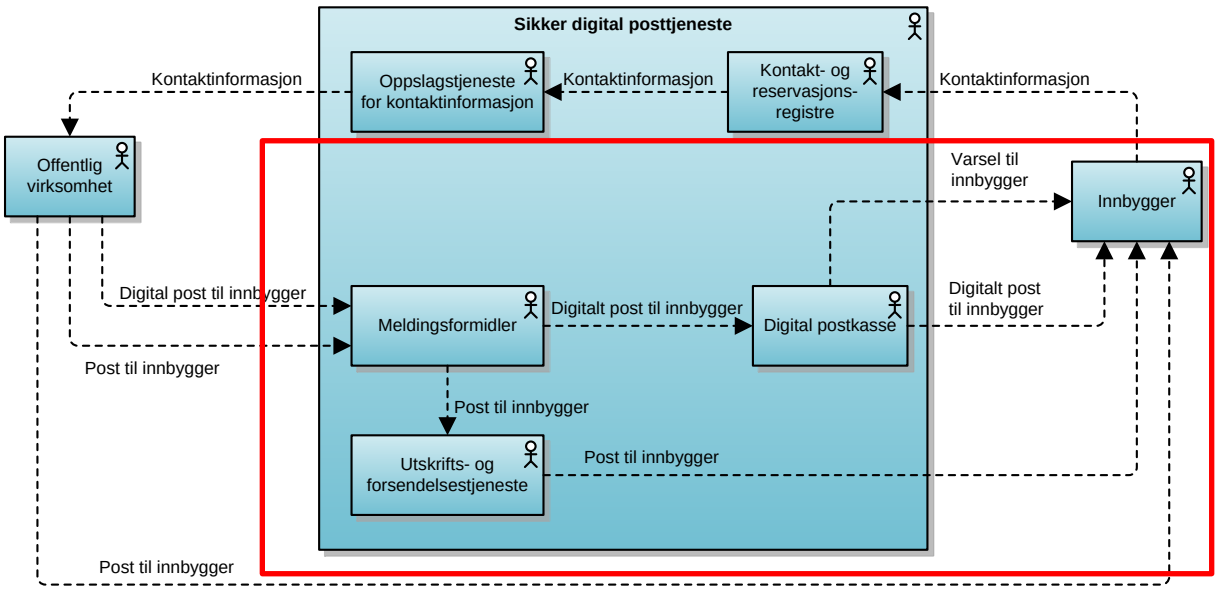
Første del av ROS-analysen var å etablere en kontekst for selve risikoanalysen. Andre del er å forstå hvilke risikoer som verdier i systemet utsettes for, og komme med forslag til tiltak for å redusere risiko.

ROS-prosjektet har diskutert og dokumentert opplevelse av trusler og sårbarheter, sannsynligheter og konsekvenser for derigjennom å kunne strukturere denne informasjonen i en ROS-analyse, hvoretter risiko kan evalueres og risikoreduserende tiltak foreslås. Knytningen mellom prosjektets arbeid og standarden er søkt klargjort ved henvisninger i rapporten, slik at det skal være lett å verifisere at alle aktivitetene omtalt i standarden er behandlet. Denne tilnærmingen vil også forenkle senere oppdateringer av ROS-analysen.

1.2.1 Scope

Denne rapporten omfatter ROS-analyse av Digital postkasse til innbyggere.

Rapporten redegjør for grunnleggende trekk ved Digital postkasse til innbyggere, avklarer involverte aktører, og redegjør for trusselbildet. Den angir også akseptert risiko og gir anbefalinger på hvilke sikkerhetstiltak som bør iverksettes for å styre et gitt risikoscenario til akseptabelt nivå.



Figur 2 Scope for ROS-analyse av Digital postkasse til innbyggere

1.2.2 Avgrensninger

Risiko internt hos avsendervirksomheten inngår ikke i analysen, herunder at meldinger adresseres til feil person eller at utro tjenere i avsendervirksomheten kopierer meldinger. Noen av risikoene som avdekkes i rapporten bør håndteres med tiltak hos avsendervirksomhetene. Dette vil komme klart frem av tiltakslisten.

Prosessuell, organisatorisk og avtalemessige risiko relatert til avtaleforhold mellom Difi, postkasseleverandør, avsendervirksomheten, e-ID utstedere og andre er ikke inkludert i analysen.

Sluttbrukers risikoappetitt er ikke inkludert. Vurderingen av risiko knyttet til angrep hos/via sluttbruker gir særlige utfordringer på grunn av at miljøet varierer fra sluttbruker til sluttbruker og det i hovedsak ligger utenfor posttjenestens kontrollsfære. Denne risikoen er derfor vurdert for seg, se kapittel 4.2.

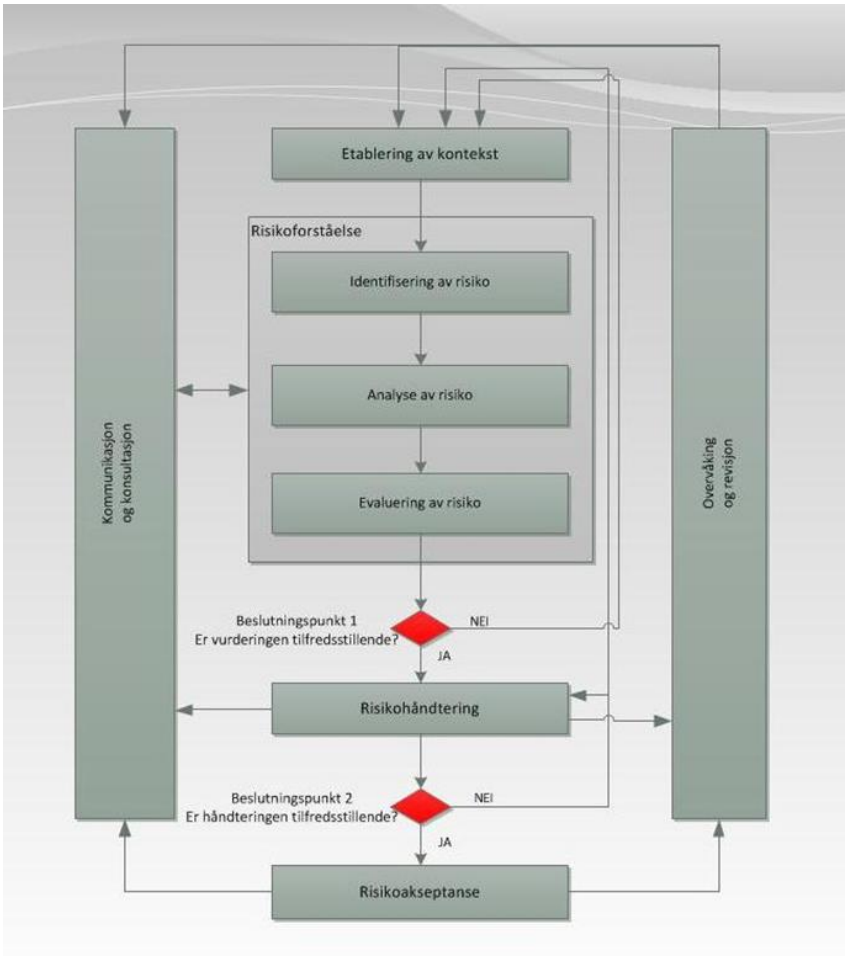
Videre har vi sett bort fra at omkringliggende systemer som ID-porten, kontakt- og reservasjonsregister som helhet er kompromittert. Det er utført egen ROS-analyse for kontakt- og reservasjonsregisteret.

2 Risikoforståelse

Målet med å skaffe frem en forståelse av risikoene i systemet er å kunne iverksette de riktige tiltakene. Stegene for å etablere forståelse av risiko følger av standardens kapittel 8.1 og består av tre trinn:

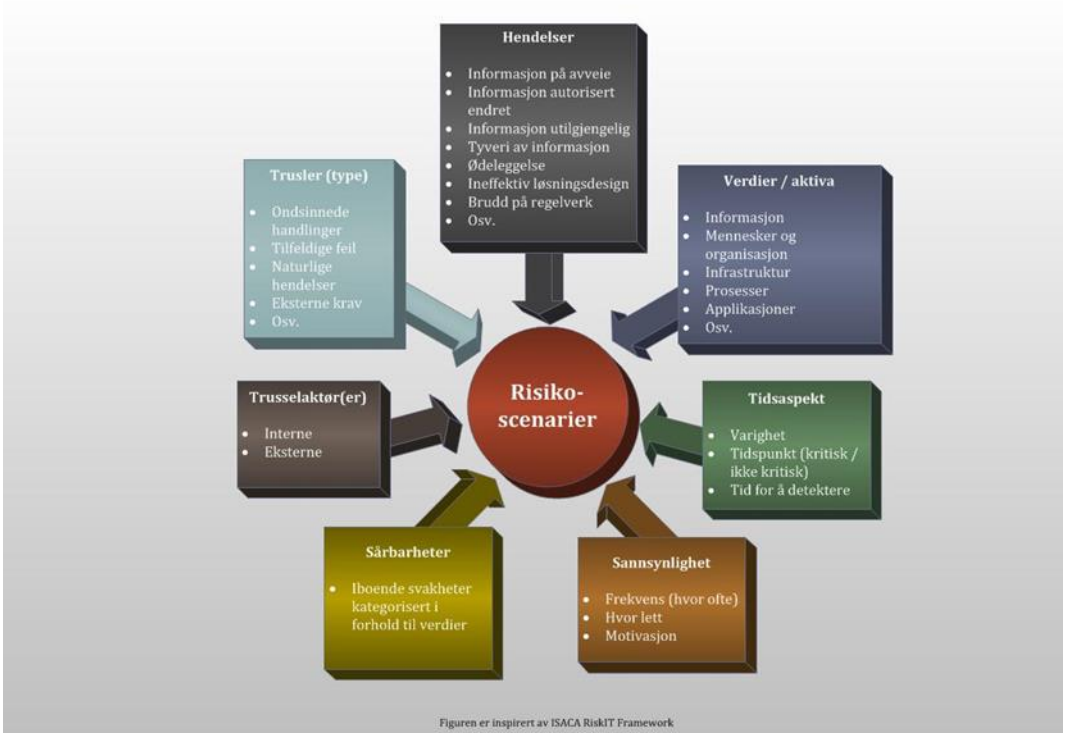
1. Det identifiseres risikoer som utsetter verdiene for fare. Risiko oppstår som en følge av en uønsket hendelse, enten direkte eller indirekte.
2. Risikoen analyseres ved å bestemme risikonivået. Nivået uttrykkes som en kombinasjon av konsekvens av en uønsket hendelse og sannsynligheten for at den skal inntreffe.
3. Risikonivået evalueres opp mot virksomhetens akseptable risiko.

En meningsfylt risikoforståelse forutsetter en veldefinert kontekst. Konteksten inneholder ikke bare kriteriene for risiko, konsekvens og så videre, men også en systemmodell og beskrivelse av hvilke verdier som står på spill. Konteksten beskrives både i de innledende kapitlene samt under hvert av de relevante kapitlene i denne ROS-analysen. Å anvende en scenario-basert metodikk i trinn 1-3 kan forenkle gjennomføring av ROS-analysen og oppfølgning i etterkant. Analysen som ligger til grunn for denne rapporten er scenario-basert.



Figur 3 Prosess for ROS-analyse, jf. ISO/IEC 27005:2011

Ettersom risikoene vil bli ordnet etter hvor alvorlige de er, legges det til rette for å iverksettes tiltak i riktig rekkefølge. Dersom restrisikoen vurderes å være for stor etter at rimelige tiltak er iverksatt, må det gjennomføres en ny runde. Dette er i tråd med standarden.



Figur 4 Elementer i risikoscenarioer

Selv om risiko, i teorien, oppstår i møtet mellom en verdi og en uønsket hendelse så er bildet naturligvis mer komplisert. Som vist i «Figur 4 Elementer i risikoscenarioer» påvirkes risikoen av mange forskjellige elementer.

Når det gjelder uønskede hendelser, deres årsaker og konsekvenser, så kan samme situasjon beskrives på forskjellige måter. For eksempel kan man si at *lekkasje av informasjon* er en uønsket hendelse, og at det kan skje som en følge av at *et varsel eller melding er sendt til en gal adresse*. Alternativt, og likeverdig, kan man si at *et varsel eller melding som kommer på avveie* er en uønsket hendelse og at konsekvensen er *at informasjon lekker ut*. Til syvende og sist er man opptatt av hva resultatet er for den som eier verdien (tap av omdømme, brudd på lov eller forskrift, brudd på ønsket / pålegg om konfidensialitet, og så videre). I dette tilfellet vil informasjonslekkasjen omfatte meldingen og varselet.

Resultatet av arbeidet med risikoforståelse er en oversikt over risikoer, prioritert i henhold til kriteriene som er fastlagt.

2.1 Identifisering av risiko

Behovet for å identifisere risiko følger av standardens kapittel 8.2.

ROS-analyser skal besvare (minst) tre spørsmål:

1. Hva kan gå galt?
2. Hvor sannsynlig er det at dette går galt?
3. Hva blir konsekvensen hvis det som kan gå galt går galt?

Hensikten med å identifisere risiko er å finne «ting» som kan skje, som igjen kan føre til et potensielt tap/skade og så undersøke hvor og hvordan et slikt tap/skade kan oppstå. Deretter lokaliserer man eksisterende mottiltak og deres innvirkning på risikoen. Til slutt vurderer man konsekvensen(e).

Risiko blir identifisert gjennom en prosess i fem steg som går ut på å identifisere:

1. Verdier
2. Trusler
3. Eksisterende tiltak
4. Sårbarheter
5. Konsekvenser.

Det er hverken nødvendig eller ønskelig å gjennomføre de fem delene sekvensielt. Disse aktivitetene kan for eksempel konsolideres med støtte i en scenario-basert metodikk.

2.1.1 Identifisering av verdier

Identifisering av verdier følger av standardens kapittel 8.2.2. En verdi er alt som anses som verdifullt for en virksomhet.

Analysedelen, kapittel 3, inneholder en oversikt over verdiene tilknyttet Digital postkasse til innbygger (punkt 3.1).

2.1.2 Identifisering av trusler

Identifisering av trusler følger av standardens kapittel 8.2.3. En trussel er et potensiale for at en verdi kan påvirkes negativt.

Trusler kan være naturlige (flom) eller resultatet av en menneskelig handling, de kan komme innenifra eller fra utsiden av tjenesten, med eller uten hensikt, som en (indirekte) følge av et uhell, og så videre. Noen trusler påvirker flere verdier og noen trusler fører til kjeder av uønskede hendelser.

En *trusselaktør* er den eller det som genererer trusselen, eller sagt på en annen måte; det eller den som utnytter en sårbarhet/svakhet ved systemet og dermed skaper en uønsket hendelse. En trusselaktør behøver altså ikke være et menneske, eller for den saks skyld en som handler med overlegg.

2.1.3 Identifisering av eksisterende og planlagte tiltak

Identifisering av eksisterende og planlagte tiltak følger av standardens kapittel 8.2.4. Tiltak benyttes for å kontrollere risiko.

Standarden slår fast at planlagte tiltak skal sidestilles med eksisterende tiltak.

Eventuelle eksisterende tiltak eller risikohåndteringsplaner skal identifiseres og dokumenteres. For virksomheten kan dette være eksisterende kriseløsninger dersom de regulære virksomhetsprosessene av en eller annen grunn gjøres uvirksomme. Et eksempel på dette kan være at man har etablert manuelle eller automatiske utsendelses- eller oppslagsløsninger som kan tre i kraft dersom digitale løsninger feiler.

2.1.4 Identifisering av sårbarheter

Identifisering av sårbarheter følger av standardens kapittel 8.2.5. En sårbarhet er en iboende svakhet.

Med utgangspunkt i identifiserte trusler, de identifiserte verdiene og alle eksisterende og planlagte tiltak søker man å identifisere sårbarheter. En sårbarhet kan ikke i seg selv skade en verdi, dette kan først skje dersom det eksisterer en trussel som kan utnytte sårbarheten. Det er derfor viktig å ha både verdiene og truslene som bakteppe når sårbarheter skal identifiseres.

Det er laget en oversikt over hendelser som er knyttet til sårbarhetene som er relatert til de verdiene som er identifisert, de truslene som er identifisert og eventuelle tiltak som er implementert.

2.1.5 Identifisering av konsekvenser

Identifisering av konsekvenser følger av standardens kapittel 8.2.6. En konsekvens er en skade på noe av verdi (omdømme, liv og helse, økonomi) som resultat av en uønsket hendelse hvor en sårbarhet er utnyttet av en trussel.

Konsekvenser beskrives som resultatet av et risikoscenario. Målet er altså å identifisere mulige konsekvenser.

Uønskede hendelser grupperes i tre kategorier:

1. brudd på konfidensialitet,
2. brudd på integritet,

3. brudd på tilgjengelighet

Disse vil igjen kunne ha følgeskader som for eksempel tap av omdømme, tap av liv og helse og økonomiske tap. Hvor alvorlig en uønsket hendelse er, vil variere med verdien.

Resultatet etter gjennomført identifisering er en liste av risikoscenarioer med deres konsekvenser, og hvordan de er relatert til verdier.

3 Analyse av risiko

Analyse av risiko følger av standarden kapittel 8.3. Formålet er å danne seg et bilde over de forskjellige hendelsesscenariene som er relevante, for dermed å lage et grunnlag for videre evaluering og behandling.

3.1 Oversikt over verdier

Det er utelukkende én verdi som avsendervirksomheten overlater til Digital postkasse til innbyggere, og det er informasjon som direkte eller indirekte inneholder opplysninger om innbyggere, deres helse og familie, økonomiske forhold, og så videre.

Avsendervirksomheten har i tillegg tre andre verdier som direkte kan påvirkes av at informasjon sendes gjennom Digital postkasse til innbyggere:

1. Innbyggerens liv og helse.
2. Sitt eget omdømme.
3. Økonomiske verdier.

Verdiene kan oppsummeres i følgende tabell:

Verdi	Beskrivelse
Innbyggers opplysninger	De samlede opplysningene om innbygger som sendes gjennom tjenesten og samles i innbyggers digitale postkasse.
Innbyggers liv og helse, omdømme og økonomi	Deler av forvaltningen vil påvirke innbyggerens liv og helse, omdømme og økonomi. Dette blir da en verdi som virksomhetene må verne om.
Virksomhets omdømme	Dette er innbyggernes oppfattelse av og forventninger til virksomhetens tjenester, troverdighet, handlekraft, og evne til gjennomføring.
Virksomhets økonomi	Virksomhetens økonomiske tap eller gevinster.

3.2 Kriterier for risikoaksept

Behovet for å fastsette kriteriene for risikoaksept følger av standarden kapittel 7.2.4.

Risiko er sannsynlighet i kombinasjon med konsekvens. Satt sammen blir det en risikomatrise. Risikomatrisen nedenfor er lagt til grunn i denne ROS-analysen og er basert på et eksempel i Faktaark 5[3].

[3] http://www.helsedirektoratet.no/lover-regler/norm-for-informasjonssikkerhet/dokumenter/faktaark/Documents/faktaark-5-fastsette-akseptkriterier.pdf

Sannsynlighet/ konsekvens		Ubetydelig	Moderat	Alvorlig	Kritisk
		1	2	3	4
Sannsynlig Hendelsen inntrer daglig eller oftere	4	4	8	12	16
Mulig Hendelsen inntrer en gang i måneden	3	3	6	9	12
Mindre sannsynlig Hendelsen inntreffer årlig	2	2	4	6	8
Sjelden Hendelsen inntreffer omkring hvert 5. år eller sjeldnere	1	1	2	3	4

Tabell 1 Risikomatrise

Nivåene for risikoaksept blir da som følger:

Lav risiko	1 – 3	Ingen tiltak nødvendig
Moderat risiko	4 – 9	Hendelsene skal vurderes nærmere og eventuelle tiltak implementeres eller risiko aksepteres
Høy risiko	10– 16	Tiltak skal iverksettes

Tabell 2 Kriterier for akseptabel risiko

Graderingen tas bare som et utgangspunkt. En må i hvert enkelt tilfelle vurdere risiko opp mot fordelene. For eksempel kan det vurderes som akseptabelt å ta en høy(ere) risiko i en overgangsperiode.

Ulike virksomheter vil ha ulike kriterier for hvilken risiko de er villig til å akseptere, da dette avhenger av hver virksomhets policyer, mål og hvilket regelverk de er underlagt. Nivåene for hver enkelt virksomhet fastsettes av ledelsen, og vil blant annet bero på følgende:

- Virksomhetsspesifikke kriterier; for eksempel er helsesektoren underlagt Normen og vil vurdere et sikkerhetsregime i tjenesten med den som målestokk.
- Lovmessige og regulatoriske aspekter vil kunne variere mellom virksomhetene.

- Operasjonelle aspekter.
- Teknologiske aspekter, for eksempel bruk av en eksisterende portal-løsning.
- Økonomi.

3.3 Trusler

Når det gjelder identifisering av utilsiktede og naturlige trusler har vi ikke identifisert noen utover de som er beskrevet i standarden. Vi antar at trusselbildet på dette området i stor grad vil være sammenfallende med truslene mot virksomhetenes systemer.

3.4 Trusselaktører

Trusselaktører er ikke like, og det finnes mange metoder for å kategorisere ulike trusselaktører. Her har vi valgt å fokusere på de samme egenskapene som i risikohåndterings-guiden til NIST, SP 800-304, og lagt til utholdenhet:

- Evne - En aktørs tilgang på kompetanse og ressurser.
- Vilje - En aktørs grad av motivasjon for å angripe.
- Målrettethet - En aktørs grad av målrettethet mot brukere eller brukergrupper. Målrettethet vil øke risikoen for individene angrepet rettes mot, pga økt frekvens og tilpasning av angrepene.
- Utholdenhet - En aktørs evne til å opprettholde et angrep over tid og evnen til å utføre flere angrepsforsøk over tid.

[4] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

De viktigste trusselaktørene vurderes slik:

Trusselaktør	Evne	Vilje	Målrettethet	Utholdenhet
Fremmed makt	5	2	5	5
Organisert kriminalitet	4	3	5	4
Hacktivister	4	3	1	2
Hacker	4	3	3	4
Media	3	3	5	4
Utro tjener i virksomheten	3	3	5	3
Utro tjener hos Difi	3	3	5	3
Utro tjener hos tredjepart/databehandler	3	3	5	3
Nærstående med fysisk tilgang	3	4	5	4
Nærstående uten fysisk tilgang	2	4	5	4
Forfølgere av trusselutsatte	2	3	5	4

Skala for evne, vilje og utholdenhet er:

5 Meget høy
4 Høy
3 Middels
2 Lav
1 Meget lav

Skala for målrettethet er:

5 Et spesifikt individ
3 En eller flere individer
1 Generisk angrep ikke spesielt rettet mot bestemte individer

Skalaene og verdiene er tidligere benyttet i ROS1 på bakgrunn av tilbakemeldinger fra bl.a. Politiet, Kripos, NAV, SPK, Helsedirektoratet og åpne kilder som PST's og NSM's trusselvurderinger, men justert på bakgrunn av erfaringene fra ROS-analysen for kontakt og reservasjonsregisteret og dialogen med oppstartsvirksomhetene, referansegruppen og leverandørene til Digital postkasse til innbygger.

Vi har lagt følgende antagelser om motivasjon til grunn for de ulike trusselaktørene:

Fremmed makt

Her er det lagt til grunn at fremmed makt vil ha både evne og vilje til å skaffe seg informasjon om personer i Norge, både personer i maktposisjoner og mot landets dissidenter/politiske aktivister. Vi viser til PSTs Åpen trusselvurdering 2013:

Etterretningsvirksomheten mot Norge og norske interesser pågår kontinuerlig, på et stabilt høyt nivå, og retter seg mot et bredt spekter av mål. Vi forventer at virksomheten særlig vil rette seg mot sikkerhets- og beredskapsmål, samt mot teknologiske, økonomiske og politiske mål. I tillegg vil flere stater opprettholde sin flyktningspionasje i Norge og forsøke å kartlegge, true og skremme dissidenter og politiske aktivister som oppholder seg her.

Organisert kriminalitet

Det er lagt til grunn at organisert kriminalitet i hovedsak retter seg mot økonomiske interesser, og at informasjonen som ligger digital postkasse til innbygger kan brukes som et ledd i ID-tyveri og lignende. I tillegg kan informasjonen brukes i forbindelse med represalier ift. Trusselutsatte innbyggere.

Hacktivister

Hacktivister ønsker ofte å oppnå et politisk mål gjennom sabotasje eller offentliggjøring av informasjon.

Hackergruppe / Individuell hacker

For disse er det lagt til grunn at de kan ønske å vise at sikkerheten ikke er god nok i løsningen og at det kan gi status å hacke tjenestene, ønske om å sabotere, eller man kan ha økonomiske motiver bak handlingene.

Media

Virksomhetene har flagget media som en potensiell stor trusselaktør også i Norge. I utlandet har det forekommet hacking fra media og det finnes også ansatte hos avsendervirksomheter som har blitt forsøkt lurt fra norsk media. Media er ofte mer interessert i å påpeke at sikkerhetshull finnes enn å faktisk benytte informasjonen. Den kommersielle gevinsten gjennom økte opplagstall/besøkstall og for eksempel en enkelt journalists status er mulige beveggrunner.

Utro tjenere i virksomhetene, eller hos tredjepart/databehandler

Det er lagt til grunn at utro tjenere kan ha økonomisk gevinst (for eksempel 1000-tips til media) som årsak eller av lojalitet eller tvang/trusler fra en annen trusselaktør skaffer seg tilgang til informasjon i digital postkasse eller relaterte tjenester. Dette kan benyttes til å se om det finnes opplysninger om bestemte individer.

Nærstående med fysisk tilgang / Nærstående uten fysisk tilgang

I denne kategorien kan det være mange årsaker, den som er mest nevnt er personer med mulige hevnmotiv (for eksempel betente barnefordelingssaker osv).

Forfølgere av trusselutsatte

Hvis det finnes innbyggere som er trusselutsatte og benytter tjenesten, kan disse spores opp om informasjon som logges eller ukrypterte metadata som følger digital post røper geografisk tilhørighet.

3.5 Vurdering av sannsynlighet

Vurdering av sannsynlighet følger av standarden kapittel 8.3.3.

Vurdering av sannsynligheten for at en hendelse inntreffer har som mål å finne svar på «hvor ofte..». Svaret angis kvantitativt, og sannsynlighetsskalaen ble fastsatt under kontekstetableringen.

For hver av de uønskede hendelser som er identifisert skal man gjøre en vurdering av sannsynligheten for at hendelsen inntreffer. I mange tilfeller kan det være vanskelig å si noe om frekvens, da det ikke finnes noe godt statistisk materiale. I disse situasjonene kan man ta med en aktørs motivasjon for å gjennomføre en handling, eller hvor lett det vil være for en aktør å gjennomføre handlingen.

En integrert del av risikoaksept er å fastsette nivåer for sannsynlighet:

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
Sannsynlig at hendelsen inntreffer 4	Hendelsen inntreffer daglig eller oftere	Sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående. Det er ikke nødvendig med spesielle kunnskaper om interne forhold.	- sikkerhetstiltak er ikke etablert - krever små til normale ressurser av egne medarbeidere eller eksterne for å brytes - ikke nødvendig med kjennskap til tiltakene
Mulig at hendelsen inntreffer 3	Hendelsen inntreffer en gang i måneden	Sikkerhetsbrudd kan skje ved uaktsomhet av egne medarbeidere. Utenforstående må ha noe kompetanse, og forsettlig (bevisst eller aktivt) gå inn for å bryte sikkerhetstiltakene.	- sikkerhetstiltak er ikke fullt etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer ikke etter hensikten - egne medarbeidere trenger kun små til normale ressurser for å bryte tiltakene
Mindre sannsynlig at	Hendelsen inntreffer årlig	Sikkerhetsbrudd kan skje ved at egne	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
hendelsen inntreffer 2		medarbeidere opptrer med forsett og har en viss kompetanse. Utenforstående må opptre med overlegg og noe kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.	- sikkerhetstiltak fungerer etter hensikten - egne medarbeidere trenger små til normale ressurser og normal kjennskap til tiltakene for å bryte disse - eksterne trenger gode ressurser og god kjennskap til tiltakene for å bryte disse
Sjelden at hendelsen inntreffer 1	Hendelsen inntreffer omkring hvert 5. år eller sjeldnere	Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer med overlegg og har spesiell kompetanse eller kunnskap. Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten.	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten - krever gode ressurser og godt kjennskap av egne medarbeidere for å brytes - eksterne kan ikke omgå tiltakene

Der erfaringstall foreligger, gir disse en indikasjon på framtidig frekvens. På bakgrunn av letthets- og motivasjonsvurderingen gjengitt over, kan også forventet frekvens anslås. Til hjelp for vurderingen er det utarbeidet kriterier for letthetsbetraktninger, se over.

Det er imidlertid også verdt å være oppmerksom på at trusselaktørers gevinst av vellykket sikkerhetsbrudd vil påvirke frekvensvurderingen, jf. at verdien vil være styrende for motivasjonen. Det kan således være nødvendig å knytte et anslag over gevinsten for trusselaktøren til opplysningene som inngår i løsningen – i tillegg til taps- og skadepotensialet for virksomheten selv, innbyggeren mv., jf. konsekvenskategoriene. For motivasjonsvurderingen vises til omtalen i Datatilsynets veileder kapittel 7.3.

3.6 Vurdering av konsekvenser

Vurdering av konsekvenser følger av standarden kapittel 8.3.2.

Vurderingen tar utgangspunkt i listen av de identifiserte uønskede hendelsene, og skal gi svar på spørsmål av typen «hva er konsekvensen hvis det som kan gå galt går galt».

At verdiene i systemet er korrekt fastsatt er kritisk for en riktig vurdering av konsekvenser.

Konsekvens kan uttrykkes som økonomiske tap, tap av liv og helse, tap av omdømme, straffeansvar for virksomheten osv.

Behovet for å fastsette kriterier for konsekvens følger av standarden kapittel 7.2.3. Det benyttes fire graderinger på konsekvens:

1. Ubetydelig
2. Moderat
3. Alvorlig
4. Kritisk

Nedenfor er kriteriene som vil bli benyttet videre:

Konsekvens-matrise	**Ubetydelig**	**Moderat**	**Alvorlig**	**Kritisk**
	1	**2**	**3**	**4**
Innbygger	En mindre uleilighet, økonomisk tap som kan gjenopprettes eller tap av anseelse eller integritet gjennom kompromittering av følsomme opplysninger	Gjenopprettbart økonomisk tap eller tap av anseelse og integritet gjennom kompromittering av opplysninger den registrerte oppfatter som krenkende. Fare for skade eller helsetap.	Helsetap, uopprettelig økonomisk tap eller alvorlig tap av anseelse og integritet	Tap av liv, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap av anseelse /integritet.
Virksomhet Omdømme	Kun mindre diskusjon i organisasjonen	Avsender må forklare seg for kundene om saken. Enkeltstående presseoppslag.	Offentlig debatt, ledelsen må forklare seg for eierne eller myndigheter	Politisk debatt, betydelig økonomisk erstatning/tap
Virksomhet Økonomisk	Ubetydelige økonomiske tap	Mange små kostnader. Reduserte besparelser.	Stort økonomisk tap. Stor engangskostnad	Betydelig økonomisk erstatning/tap

Disse kriteriene er hentet fra Norsk Helsenetts veileder for risikovurdering[5] og deretter modifisert på bakgrunn av møtene med avsendervirksomhetene, interne vurderinger, og best practice.[6]

3.7 Estimering av risiko(nivå)

Behovet for å estimere risiko følger av standarden kapittel 8.3.4.

Det er lagd en oversikt over identifiserte uønskede hendelser, hva som er årsaken (sårbarhet/trussel) og mulige konsekvenser. Dette er lagt inn i et register for å sikre at man skal kunne holde oversikten og for enkelt å kunne justere vurderingen av risikoen, eksempelvis på grunn av at tiltak innføres.

Sannsynlighet og konsekvens er anslått, basert på skalaer fastsatt i Vurdering av sannsynlighet og Vurdering av konsekvens. Risiko fremkommer som et resultat av dette.

4 Evaluering av risiko

Behovet for å evaluere risiko følger av standardens kapittel 8.4.

I risikoregisteret evaluerer vi risikoene ved å trekke frem relevante scenarier og knytte disse til verdier for sannsynlighet og konsekvens. Produktet av disse gir en verdi for risiko. Ved vurdering av risiko er eksisterende og planlagte tiltak og effekten av disse på sannsynlighet og konsekvens gjenspeilet i verdiene. I tillegg er det vurdert andre mulige tiltak som kan redusere sannsynlighet eller konsekvens. Effekten av de mulige tiltakene er vurdert, og fremstilt som risiko etter tiltak. På denne måten framstår verdier for risikoene før og etter mulige tiltak og effekten av tiltakene kan måles.

I risikogruppene under har vi slått sammen risikoer med en eller flere fellestrekk. Det kan være risikoer som utløses av samme hendelser eller reduseres av samme type tiltak.

4.1 Omtale av de viktigste risikogruppene – sett fra virksomhetene og Difi

Det er ikke identifisert noen risikoscenarier med *høy* risiko (ingen «røde» risiko) ved innføringen av Digital postkasse til innbyggere. Ut fra denne risikovurderingen er det derfor ikke påkrevet å iverksette umiddelbare tiltak. ROS-analysen har således ikke avdekket forhold som kunne være til hinder for produksjonssetting planlagt til 18. november 2014.

Det er imidlertid avdekket scenarier der risiko er kalkulert som *moderat* («gule» risiko). Tiltak må derfor vurderes for å få risikoene ned på akseptabelt nivå.

---

[5] http://www.nhn.no/informasjonssikkerhet/risikovurdering

[6] Liknende/alternative konsekvenskategorier finnes hos Datatilsynet (pkt 6.2, s 14), Difi (pkt 3.2.4), Digitaliseringsstyrelsen (side 24) og NSM (pkt 3.6.2, s 25)

I dette kapittelet er funnene fra risikovurderingen gruppert i figuren nedenfor. Pilene indikerer risikogruppenes endring i risikoverdi ved gjennomføring av anbefalte tiltak. Eksisterende eller planlagte tiltak, samt anbefalte tiltak, er beskrevet i *kursiv* under omtalen av hver risikogruppe i dette kapittelet. Innbyggers risiko beskrives i 4.2.

Sannsynlighet/ konsekvens		Ubetydelig	Moderat	Alvorlig	Kritisk
		1	2	3	4
Sannsynlig Hendelsen inntrer daglig eller oftere	4				
Mulig Hendelsen inntrer en gang i måneden	3		Post utilgjengelig for mottaker		
Mindre sannsynlig Hendelsen inntreffer årlig	2	Varsling feiler	Manglende forvaltning Tjenestens egnethet Tjenesten utilgjengelig for avsender	Uberettiget tilgang til meldinger	
Sjelden Hendelsen inntreffer omkring hvert 5. år eller sjeldnere	1	Informasjonens gyldighet			Trusselutsatte oppspores Uberettiget bruk av postkassen

Trusselutsatte oppspores Meldinger som sendes til trusselutsatte kan inneholde forskjellige typer av geolokaliserende informasjon. Logger hos avsendervirksomheter og meldingsformidler kan røpe tilhørighet. For eksempel om avsendervirksomheten er lokalisert i et geografisk bestemt område slik som en liten kommune, bydelsutvalg, barnehager, legekontor og skoler.

> *Det er strenge tilgangsbegrensninger til logger og systemer som inneholder slik informasjon. Virksomhetene må selv være bevist på metadata som sendes utenfor den krypterte pakken, ved kommunikasjon til trusselutsatte, og implementere tiltak som gjør risikoen akseptabel. Et mulig tiltak for virksomheter som har avsenderadresser som kan knytte den trusselutsatte til et geografisk område, er å skjerme adressen sin bak en generell utsendingsadresse uten slik tilknytning. Dette benytter f. eks NAV seg av.*

Post utilgjengelig for mottaker – Mottaker kan være forhindret i å få tilgang til posten sin av mange forskjellige årsaker. Innbyggere kan ha problemer med e-ID, viktig post blir skjult i mengden, eller ved en feil sletter innbyggeren innhold i sin postkasse. Postkasseleverandørene kan ha nedetid, eller feil

som gjør at postkassene er utilgjengelige, en postkasseleverandør kan gå konkurs, eller legge ned, eller endre på bruksvilkårene, slik at innbyggere som ikke godtar de nye vilkårene vil miste tilgang til postkassen. Virksomhetene kan sende eller adressere post feil, slik at post ikke kommer frem til rett mottaker.

Innbyggerne må selv sørge for at man har en gyldig e-ID. ID-porten sørger for at det er mulig å benytte flere forskjellige e-ID-er for å logge inn til post fra offentlig sektor. Brukergrensesnittene hos postkasseleverandørene er utformet slik at postkassene skal være enkle for innbyggerne å forholde seg til. Det er separasjon av post fra offentlige og private avsendere. Sletting av egen post er en omstendelig handling, for å unngå utilsiktet sletting. Innbygger skal varsles pr SMS eller e-post når viktig post er tilgjengelig i postkassen.

Det anses som svært lite sannsynlig at postkasseleverandørene vil undergrave sin egen markedsposisjon ved å endre på bruksvilkårene slik at kundene går over til konkurrenten. Bruksvilkår er endret og tilpasset i forkant av produksjonssetting.

Leverandørene har tiltak i form av katastrofeberedskap, dupliserte løsninger og to lokasjoner, samt backup av postkassene, for å sikre tilgjengelighet. Ved konkurs, eller nedleggelse er det kontraktsfestet at post blir overført til annen postkasseleverandør.

Det er mulig å implementere tiltak hos postkasseleverandørene som reduserer risiko i forbindelse med feilutsendelser ved at postkasseleverandørene sjekker fødselsnummer mot digital postkasseadresse før brev blir lagt i innbyggers postkasse. Virksomhetene må selv sørge for tiltak som gjør risikoen for sending av post til feil mottaker akseptabel. Det er postkasseleverandørene som registrerer innbyggernes postkasseadresser i kontakt- og reservasjonsregisteret, slik at innbygger ikke skal sette feil verdi for denne.

Uberettiget tilgang til meldinger. Flere scenarier kan gi uberettiget tilgang til meldinger. Det kan være tyveri eller misbruk av e-ID (f eks ut over en gitt fullmakt), eller feil videresending fra brukers side. Utro tjenere, falske meldingsformidlere, fremmed makt eller hackere kan også forsøke tilegne seg tilgang til en innbyggers post. I tillegg kan post sendes til feil mottaker, som også vil gi uberettiget tilgang til informasjonen.

Leverandørene har strenge tilgangsbegrensninger. Det er implementert sporing på handlinger som kan påvirke innbyggernes informasjon og for å bryte med regimet trengs det flere utro tjenere som samarbeider. Leverandørene følger prinsipper for sikkerhet i flere lag, regelmessig penetrasjonstester og andre sikkerhetstester. Det er også etablert overvåkings-/monitoreringstjenester. Meldingsformidleren har hvitliste med aktuelle postkasseleverandører for å hindre falske postkasseleverandører i løsningen.

Brukergrensesnittet i de forskjellige løsningene skal være enkle for innbyggerne å forholde seg til. Det er separasjon av post fra offentlige og private avsendere. Det finnes også brukerveiledninger hos postkasseleverandørene, som innbyggerne kan benytte seg av.

Tiltak som forhindrer feilutsendelser og feiladressering må vurderes og implementeres hos virksomhetene.

Tjenesten er utilgjengelig for avsender - Det kan være mange årsaker til at tjenesten blir utilgjengelig. Det kan være at ytelsen i løsningen ikke er god nok for å håndtere uventete trafikktopper, eller at tjenesten utsettes for tjenestenektangrep, feil i virksomhetens egne systemer eller feil i et punkt i leveransekjeden til tjenesten.

Kapasitetsplanlegging, beredskapsplaner og tekniske tiltak hos Difi og leverandørene er etablerte tiltak som motvirker og begrenser effekten av slike hendelser.

Virksomhetene må selv sørge for tiltak for å sikre tilgjengelighet i de komponentene som er innen for deres kontroll.

Manglende forvaltning – Risiko som er knyttet til manglende rutiner og prosesser rundt tjenesten. Dette kan være manglende rutiner for varsling av feil, eller vedlikehold, eller lav bevissthet rundt kritiske utsendelser til de forskjellige aktørene som benytter seg av tjenesten Digital postkasse til innbyggere.

Prosesser og rutiner er utarbeidet og vil bli tatt i bruk i godkjenningsperioden. Difi vil vedlikeholde en kalender som viser de forskjellige virksomhetenes kritiske utsendelser. Det vil bli varslet feil og vedlikehold via samarbeidsportalen.

Virksomhetene må på sin side ha rutiner på plass for å håndtere planlagt nedetid og varsling av store forsendelser.

Uberettiget bruk av postkassen (til ikke-forvaltningsmessig formål). En uberettiget utsending kan misbrukes til spam, markedsføring, spre et budskap mv. Dette forutsetter at en autorisert bruker opptrer som en utro tjener. Ved virus i virksomhetene kan dette spres via PDF-dokumenter eller lignende, tilsiktet eller utilsiktet.

Det er implementert tiltak som tillater virksomhetene å sette volumsperre ift. forventet volum av utsendelser. Det er sikkerhetsovervåkning på plass som raskt vil avdekke misbruk og som vil være avskrekkende. For private aktører som misbruker sin rolle som avsender på vegne av det offentlige, vil misbruk få konsekvenser som utestengelse og evt. erstatningsansvar.

Postkasseleverandørene vil ikke gi ut informasjon fra sine logger til virksomhetene, som kan brukes til sporing av innbyggere. Unntaket er åpningsbekreftelse som ikke sendes uten at innbyggeren informeres og godtar det, eller utlevering av informasjon som følge av rettslig pålegg.

En av postkasseleverandørene har implementert anti-virus, som kan stoppe spredning gjennom postkassen.

Virksomhetene bør på generell basis sørge for beskyttelse mot virus og skadevare

Tjenestens egnethet – Dette er en risiko som går på at man ikke direkte kan ta den posten som sendes per brev i dag og digitalisere denne med ønsket resultat. Et eksempel er skjemaer som skal fylles ut og sendes tilbake. Det vil være forskjellig utstyr hos innbyggerne og noen har ikke mulighet til å skrive ut skjemaer og sende disse tilbake.

> *Tiltak for å gjøre prosessene rundt kommunikasjonen med innbyggere digital og hensiktsmessig for både utsendelse og innsendelse, må implementeres hos virksomhetene.*

Varsling feiler. Selv om meldingene blir levert, kan varselet om meldingen utebli ved feil på tjenestene for utsending av SMS eller epost.

> *Dersom meldingen ikke er åpnet etter sju dager fra første varsel ble sendt, vil postkassen repetere varselet. Virksomhetene vil også få et varsel om at varsel ikke er levert, dersom dette kan avdekkes av postkasseleverandøren. Utover dette er det ikke identifisert noen tiltak utover at varsel kan sendes som SMS og epost, der innbyggeren er registrert med begge deler.*

Informasjonens gyldighet – Risiko forbundet med å bevise at et dokument er ekte og uendret.

> *Integritetsbeskyttelse er godt ivaretatt i løsningen. Alle dokumentpakker som sendes igjennom Digital post til innbyggere er signert med avsendervirksomhetens sertifikat. Signaturen følger dokumentet og vil bli ugyldig ved endringer på dokumentet. Denne signaturen følger også dokumentet om man flytter post i mellom postkasseleverandørene. Virksomheten må følge ordinære retningslinjer for arkivering.*

4.2 Risikovurdering for innbyggere

Nedenfor beskrives de alvorligste risikoene som innbygger må akseptere:

Sannsynlighet/ konsekvens		Ubetydelig	Moderat	Alvorlig	Kritisk
		1	2	3	4
Sannsynlig Hendelsen inntrer daglig eller oftere	4	Varsling feiler			
Mulig Hendelsen inntrer en gang i måneden	3		Uberettiget tilgang til meldinger		
Mindre sannsynlig Hendelsen inntreffer årlig	2				
Sjelden Hendelsen inntreffer omkring hvert 5. år eller sjeldnere	1				Post utilgjengelig for mottaker

Post utilgjengelig for mottaker – En del av risikoen rundt utilgjengelig post er knyttet til feil på e-ID, innbygger har mistet tilgang til sin e-ID, eller gitt andre for vide fullmakter, slik at man ikke får tilgang til egen postkasse eller at brev blir slettet av personen med fullmakt. Brukerfeil som fører til sletting/deaktivering av postkassen kan også forekomme.

> *Innlogging via ID-porten gir mulighet for å bruke flere e-ID-er (BankID, Buypass, Commfides og minID). Det bør vurderes informasjonstiltak om fullmaktsbruk av e-ID veiledning om hvordan innbygger kan få sperret e-ID-en. Sletting av postkassen er en veldig omfattende prosess, for å unngå utilsiktet handling.*

Uberettiget tilgang til meldinger. Meldinger kan leses av personer som har tilegnet seg tilgang til en brukers e-ID eller ved at innbygger har gitt tilgang/fullmakt til noen som leser meldingen. Innbygger kan også videresende meldinger ved en feil, og mottaker kan lese meldingen.

> *Innbygger må selv få sperret sin e-ID. Innbygger må også sette seg inn i bruken av sin valgte postkasse, slik at man er kjent med brukergrensesnitt og fullmaktsbruk. Postkasseleverandørene har brukerveiledninger for sine løsninger.*

Varsling feiler. Selv om meldingene blir levert, kan varselet om ny post utebli ved feil på innbyggerens side som forhindrer at varselet blir levert, slik som feil på eposttjeneste, eller problemer med mobiltelefontjenesten til innbyggeren.

> *Dersom meldingen ikke er åpnet etter sju dager fra første varsel ble sendt, vil postkassen repetere varselet. Virksomhetene vil også få et varsel om at varsel ikke er levert, dersom dette kan avdekkes av postkasseleverandøren. Utover dette er det ikke identifisert noen tiltak utover at varsel kan sendes som SMS og epost, der innbyggeren er registrert med begge deler.*

5 Avvik

I skrivende stund (november 2014), er e-Boks forsinket og ikke klar for å lansere tjenesten. Digital postkasse for innbyggere vil derfor bli produksjonssatt kun med én digital postkasse – Digipost. e-Boks vil bli koblet til så snart de er klare og akseptansetesten er godkjent, tentativ i februar 2015. Dette har medført at prosjektet ikke har fått verifisert at alle sikkerhetskravene og tiltakene regulert i kontrakten, er implementert hos e-Boks. Denne gjennomgangen vil bli gjort i forbindelse med akseptansetesten. Hvis det da finnes vesentlige avvik, må relevante risikoer revurderes og denne rapporten justeres.

Digipost har tre utestående punkter som et resultat av testing, og gjennomgang av sikkerhetskrav og sikkerhetstiltak. Dette dreier seg om dreier seg om tekniske komponenter som skal være på plass før løsningen settes i drift og dokumentasjon som skal fremlegges innen utløpet av godkjenningsperioden.

6 Sluttord

Når digital postkasse til innbygger blir produksjonssatt, 18. november 2014 vil Digiposts kunder (ca 370.000) begynne å motta digitale brev fra offentlig sektor gjennom løsningen. De første virksomhetene som tar tjenesten i bruk, oppstartsvirksomhetene, er Statens Innkrevingssentral, NAV, Kreftregisteret og KS SvarUt/Bergen kommune. Flere offentlige virksomheter kommer raskt etter. Det forventes at leverandørene øker sine markedsaktiviteter overfor innbyggerne og bidrar til å få mange innbyggere til å velge seg en digital postkasse. Denne analysen ser på risikoer som oppstår ved at flere offentlige virksomheter går over til å kommunisere med innbyggerne digitalt og ikke på papir. En økende mengde informasjon om innbyggerne vil dermed lagres på samme sted. Risikoer som følge av dette er også vurdert.

Denne risikoanalysen bygger på utstående risikoer fra ROS1 og restrisiko for disse vurdert i lys av inngåtte kontrakter og etablerte tiltak i Difis forvaltning av denne nye felleskomponenten. Det er gjennomført arbeidsmøter med oppstartsvirksomhetene og med en referansegruppe[7] bestående av virksomhetene i styringsrådet for Difis felleskomponenter og virksomhetene som deltok i ROS1. Disse har hatt innsyn i arbeidet med analysen og har kommet med innspill til ROS-arbeidet i form av nye risikomomenter. Tilbakemeldingen fra virksomhetene er et generelt inntrykk av at det er gjort mange gode tiltak for å redusere risikoen.

I denne ROS-analysen av Digital postkasse til innbyggere er det ikke avdekket noen risikoscenarier med høy risiko («røde» risiko), risikoer der produktet av sannsynlighet og konsekvens er større enn ni og krever umiddelbare tiltak. Det er imidlertid avdekket scenarier der risiko er kalkulert som moderat («gule» risiko). Tiltak må derfor vurderes for å få risikoene ned på akseptabelt nivå.

Virksomhetene må foreta sin egen vurdering med tanke på den informasjonen de skal sende igjennom løsningen, og selv vurdere om det er trusselaktører som er særlig ute etter disse opplysningene. Vurderingen bør ta hensyn til om risikobildet er endret i særlig grad i forhold til utsending av post på papir. Til eksempel vil man i Digital postkasse til innbyggere vite at et brev er levert i postkassen til innbyggeren, noe man ikke vet om post på papir.

Det følger av standardens kapittel 12.2 at styring av risiko er en iterativ prosess hvor risiko kontinuerlig skal monitorers, revideres, og forbedres. Ettersom tjenesten videreutvikles eller får betydelige endringer, bør risiko-analysen oppdateres. ROS-analysen bør revideres regelmessig, anslagsvis en gang i året.

[7] Følgende virksomheter har deltatt i referansegruppen: Skatteetaten, NAV, Brønnøysundregistrene, Lånekassen, Samordna opptak, KS/KommIT, Politidirektoratet, Statens Pensjonskasse, Helsedirektoratet, Bergen kommune