

Risikovurdering - en veiledning til Rammeverket for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor

Forord

Fornyings- og administrasjonsdepartementet lanserte i april 2008 retningslinjer for offentlige virksomheter som tilrettelegger elektroniske tjenester og samhandling på nett (Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor).

Dette er en veileder til Rammeverket. Veiledningen gir en innføring i gjennomføring av risikovurderinger for offentlige virksomheter, og skal lede fram til valg av riktig sikkerhetsnivå og sikkerhetsløsninger ved bruk av IKT i samhandlingen med enkeltmennesker og næringslivet.

Oslo 29. januar 2010

Hans Christian Holte
direktør

Innhold

1	Innledning	1
1.1	Rammeverket og Kravspesifikasjon PKI	2
1.2	Målgruppe	3
2	Risikovurderinger	5
3	Gjennomføring av risikovurderinger	7
3.1	Forberedelsesfasen	9
3.1.1	Anbefalt prosess	11
3.2	Helhetlig risikovurdering	11
3.2.1	Kartlegging av verdier	12
3.2.2	Identifisere uønskede hendelser	14
3.2.3	Årsak	16
3.2.4	Sannsynlighet og konsekvens.....	17
3.2.5	Beskrive avdekket risiko	22
3.2.6	Analysere og vurdere tiltak	22
4	Anbefalte tiltak	25
4.1	Preventive og reaktive tiltak.....	25
4.2	Risikostyring - suksesskriterier	25
5	Revisjon og kontroll	27
6	Metode og kilder	29
	Vedlegg 1 - Relevante lover og forskrifter	31
	Vedlegg 2 - Anbefalinger	33
	Vedlegg 3 - Forslag til skjema og utfyllingsveiledning.....	35

1 Innledning

God informasjonssikkerhet forutsetter kunnskap om risiko- og mulighetsbildet. For kunne prioritere riktig og begrunne sine valg, eventuelt manglende valg, av sikkerhetstiltak, må virksomheten først ha oversikt over egne oppgaver og verdier, hvilke regler som gjelder og hvilke trusler de står overfor. Sikkerhetstiltak kan avverge og forebygge trusler, men også gjøre løsninger mulig som ikke ellers ville vært mulig.

Denne veiledningen er til [Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor](#)¹ (Rammeverket). Offentlige virksomheter bør gjennomføre risikovurderinger ved etablering av nye elektroniske tjenester eller samhandling, og ved revidering av eksisterende. I den sammenheng skal virksomhetene kunne vurdere risikonivået i en elektronisk tjeneste opp mot de felles definerte risikonivåene i Rammeverket. Virksomheten kan så finne anbefalte sikkerhetsnivå og implementere en autentiserings-/ uavviselighetsløsning i henhold til dette nivået (autentisering basert på elektronisk ID).

I Rammeverket er begrepet autentisering beskrevet som verifikasjon av påstått identitet (identitetskontroll), og begrepet uavviselighet som bekreftelse av at en handling eller informasjonselement er uendret og at det kan knyttes til en bestemt identitet (bevissikring).

Risikovurderinger bør gjennomføres av alle informasjonssystemer i offentlig og privat sektor. Risikovurderingsprosessen er et verktøy for en systematisk gjennomgang av sikkerheten i virksomhetens informasjonssystemer. Basert på resultatene fra vurderingen kan det iverksettes tiltak som reduserer risikoen.

Det er viktig å være bevisst på hva risikovurderingene knytter seg til; hele eller deler av virksomheten som sådan, behandlingen av personopplysninger i seg selv, eller forvaltningens og brukers identitet og handlinger (autentisering og uavviselighet). Alt kan ikke risikovurderes under ett, men mye må ses i sammenheng, blant annet ut fra tanken om at en kjede ikke er sterkere enn det svakeste leddet. Metodikken for risikovurdering vil imidlertid i stor grad være den samme, selv om objekt for risikovurdering varierer.

Det finnes flere gode veiledninger i risikovurdering generelt og innen konkrete fagområder. Denne veiledningen er rettet mot offentlig sektor, særlig i forbindelse med bruk av fellesløsninger for elektronisk ID (eID). Veiledningen inneholder ikke nye krav, men anbefaler en fremgangsmåte for å oppfylle eksisterende forpliktelser.

¹ Se: <http://www.regjeringen.no/nb/dep/fad/dok/lover-og-regler/retningslinjer/2008/rammeverk-for-autentisering-og-uavviseli.html?id=505958>

Å gjennomføre prosesser for å velge og iverksette tiltak som skal endre risiko (risikohåndtering) er pålagt i enkelte lover og forskrifter (se bl.a. [forskrift om sikkerhetsadministrasjon § 4-1](#) og NS-ISO/IEC Guide 73:2006). Forskrift om elektronisk kommunikasjon med og i forvaltningen ([eForvaltningsforskriften § 13](#)) stiller krav om utarbeidelse av sikkerhetsmål og sikkerhetsstrategi. Videre pålegger [personopplysningsloven § 13](#) den behandlingsansvarlige å sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet. I forskriften til loven er det også gitt regler om at risikovurdering må gjennomføres med sikte på å klarlegge sannsynligheten for og konsekvensene av sikkerhetsbrudd, se [personopplysningsforskriften § 2-4](#). Dokumentasjon på at risikovurdering er gjennomført skal være tilgjengelig for tilsynsorganer. Regelverket er nærmere omhandlet i [vedlegg 1](#).

- Hvilken risiko er det for bruker og forvaltning (saksbehandlingen) hvis identiteten ikke lar seg bekrefte, eller hvis det er forveksling av personer/identiteter?
- Hvilken risiko løper virksomheten hvis uvedkommende får se, endre eller slette informasjon?
- Hvilken risiko løper virksomheten hvis systemet ikke fungerer?
- Risikovurderinger skal utføres regelmessig
- Risikovurderinger gir grunnlag for å bestemme tiltak

1.1 Rammeverket og Kravspesifikasjon PKI

Rammeverket er fastsatt av Fornyings- og administrasjonsdepartementet (FAD) april 2008 og skal være et hjelpemiddel for offentlige virksomheter med å velge sikre løsninger for elektronisk kommunikasjon. FAD og KS anbefaler at både statlige og kommunale virksomheter benytter Rammeverket når det skal etablere elektroniske tjenester og samhandlingsløsninger ([se felles brev fra FAD og KS 24.4.2008](#))²

Rammeverket definerer fire sikkerhetsnivåer, og legger til rette for etablering og bruk av felleskomponenter for autentisering og uavviselighet i offentlig sektor. Disse fire sikkerhetsnivåene (nivå 1-4) har etter hvert blitt innarbeidede begreper i offentlig sektor. Med felleskomponenter menes programvarefunksjonalitet som det er et felles behov for i flere virksomheter i offentlig sektor og som disse benytter eller vil benytte i sine IKT-løsninger.

MinID og ID-porten er felleskomponenter som tilbyr elektronisk identitetskontroll (eID-tjenester) på de to høyeste sikkerhetsnivåene, nivå 3 og nivå 4. Ved at virksomheten benytter rammeverkets forhåndsdefinerte risiko- og sikkerhetsnivåer, kan den enklere vurdere hvilke felleskomponenter som dekker virksomhetens behov. Hvilket sikkerhetsnivå som er nødvendig for den aktuelle tjenesten, kan først besluttes etter gjennomført risikovurdering.

² Se: http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_brev.pdf

I vurderingen av en tjenestes totale sikkerhetsnivå må imidlertid også andre forhold vurderes, som sikring av tilknyttet utstyr (sluttbrukers og tjenesteeiers), herunder sikring av autorisasjon og tilgangskontroll til informasjon og ressurser.

Videre er det en målsetting med veiledningen å understøtte [Kravspesifikasjon for PKI i offentlig sektor](#). PKI er forkortelse for Public Key Infrastructure, en infrastruktur for offentlige nøkler. Kravspesifikasjonen er en overordnet funksjonell spesifisering for PKI-basert eID som legges til grunn ved elektronisk kommunikasjon med og i offentlig sektor. PKI-løsninger som benyttes i offentlig virksomhet skal oppfylle kravspesifikasjonen. Formålet med kravspesifikasjonen er å bidra til enklere anskaffelser og felles krav til sikre og standardiserte PKI-tjenester i forvaltningen.

Ved utarbeidelsen av Kravspesifikasjonen for PKI i offentlig sektor ble det identifisert tre sikkerhetsnivåer, to for privatpersoner og et for virksomheter ("Person-Høyt", "Person-Standard" og "Virksomhet"). Sikkerhetsnivåene i kravspesifikasjonen forholder seg til de to øverste sikkerhetsnivåene i rammeverket: nivå 3 og 4. "Person-Standard" er tilpasset krav til nivå 3, og "Person-Høyt" er tilpasset krav til nivå 4.

Kravspesifikasjonen er utarbeidet for å dekke krav til PKI-produkter og -tjeneste (elektronisk ID, signatur og kryptering) for alle typer elektronisk kommunikasjon med og i offentlig sektor, både internt i det offentlige og mellom det offentlige og enkeltpersoner eller privat næringsvirksomhet. Den enkelte virksomhet må vurdere hvilke PKI-tjenester og produkter de har behov for, og på hvilket sikkerhetsnivå.

- De to øverste sikkerhetsnivåene som beskrevet i Rammeverket svarer til sertifikatklassene beskrevet i Kravspesifikasjonen for PKI i offentlig sektor

1.2 Målgruppe

- Målgruppe: Personell involvert i i arbeidet med valg av sikkerhetsnivå, øvrige sikkerhetsrelaterte beslutninger og implementering av tekniske løsninger i offentlig sektor. Det omfatter valg av sikkerhetsnivå, øvrige beslutninger og implementering av tekniske løsninger for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor (statlig og kommunal).

Offentlige virksomheter skal jevnlig gjennomføre risikovurderinger, blant annet ved etablering av nye elektroniske kommunikasjonstjenester og ved revisjon av eksisterende. Dette gjelder uavhengig av om det gjelder egenutvikling av løsninger eller ved anskaffelser, hvor sikkerhetsnivå må vurderes og spesifiseres i kravspesifikasjonen. Hver virksomhet er selv ansvarlig for de vurderinger og valg som gjøres for å sikre egne tjenester, og eventuelle følger av disse valgene.

Ved gjennomføring av risikovurdering er det en fordel at virksomheten har en form for sikkerhetsorganisasjon / en struktur for gjennomføring og plassering av ansvar. Enhetens leder er ofte delegert ansvar for sikkerhet på sin enhet, og er derfor den som må være pådriver for gjennomføring av risikovurdering av enhetens informasjonshåndtering.

En vellykket gjennomføring av risikovurdering krever at ledelsen på enheten aktivt går inn i prosessen. Enten ved selv å lede arbeidet, eller ved at den operativt ansvarlige for risikovurderingen rapporterer til enhetsleder.

Risikovurderingsarbeidet må inkludere personell med kompetanse på riktig nivå, både rent faglig og innen IKT. Personellet bør være sammensatt slik at man kan få dekket ulike perspektiver fra flere vinkler, kunne identifisere vesentlige trusler og svakheter for de ressurstypene og situasjonstypene som vurderes. Er det begrenset intern kompetanse er det viktig å avgrense omfanget, eventuelt knytte til seg eksterne.

2 Risikovurderinger

Risikovurdering innen et område skal gi svar på:

- Hva kan gå galt? (identifisere fare)
- Hva er sannsynligheten for at det går galt? (sannsynlighetsanalyse)
- Hva er de mulige konsekvenser? (konsekvensanalyse)
- Ved å identifisere risiko og sette i verk tiltak kan problemer synliggjøres og unngås før de oppstår

Gjennomført risikovurdering kan benyttes som dokumentasjon på at virksomheten oppfyller lovkrav.

Virksomheten skal, som et ledd i den totale sikkerhetshåndtering, løpende vurdere om informasjon, og informasjonssystemene generelt, er godt nok sikret i forhold til risikobildet og kjente sårbarheter. Gjennom risikohåndtering skal virksomhetene avdekke behov for å iverksette ytterligere risikoreduserende tiltak.

Sikkerhet innebærer håndtering av risiko. Risiko uttrykker fare for tap av viktige verdier som følge av uønskede hendelser. Begrepet handler om sannsynlighet for at noe kan skje (trussel) og hvilke konsekvenser denne hendelsen eventuelt kan få. I denne veiledningen benyttes begrepet risiko som en kombinasjon av sannsynlighet for og konsekvens av en gitt hendelse. Dette samsvarer blant annet med NS-ISO/IEC Guide 73:2006. Risiko kan også defineres noe bredere, se blant annet ISO 31000:2009 som knytter begrepet til usikkerhet: "[Risk is the] effect of uncertainty on objectives".

Ved å kombinere kunnskap i en strukturert prosess skal uønskede hendelser identifiseres og rangeres etter risiko, og beskrives i systemets risikobilde (risikovurdering). (En uønsket hendelse inntreffer når informasjon og objekter kan bli kompromittert. Med kompromittering av informasjon menes her tap eller fare for tap av konfidensialitet, integritet og tilgjengelighet.) Risikovurdering er i NS-ISO/IEC Guide 73:2006 beskrevet som en samlet prosess som består av risikoanalyse og risikoevaluering. Risikovurdering gir grunnlag for å vurdere konkrete risikoreduserende tiltak knyttet opp mot de identifiserte hendelsene. Risikohåndtering utøves når sikkerhetsforanstaltninger vedlikeholdes ved løpende overvåking, justeres etter et fastlagt nivå og risikovurderinger gjentas regelmessig.

Det primære formålet med, og utbyttet av, en risikovurdering er identifikasjon og prioritering av risikoer. Resultatet av vurderingen skal inngå i ledelsens risikostyring. Risikostyring er i NS-ISO/IEC Guide 73:2006 beskrevet som koordinerte aktiviteter for å rettlede og styre en organisasjon mht. risiko. Risikostyring omfatter typisk risikovurdering, risikohåndtering, risikoaksept og risikokommunikasjon) Ledelsen skal prioritere og vedta nødvendige tiltak for å sikre at risiko er begrenset til et nivå som er akseptabelt for virksomheten. I dette ligger å bestemme hvilken risiko- og restrisiko virksomheten er villig til å leve med. Utfordringen er å etablere kontrolltiltak som er tilpasset den aktuelle risikoen slik at man får et balansert samsvar mellom rettslige rammebetingelser,

måloppnåelse, risiko og kontrollnivå. Hensikten er å finne frem til hva som er god nok informasjonssikkerhet i forhold til de konkrete utfordringene virksomheten står ovenfor. Systematiske risikovurderinger hjelper virksomheten å arbeide med de riktige tingene og gjøre tingene riktig første gang.

Informasjonssikkerhet er tradisjonelt beskrevet gjennom de tre begrepene tilgjengelighet, integritet og konfidensialitet ([personopplysningsloven § 13](#)). Med dette menes at informasjonen skal være tilgjengelig for rette vedkommende, at informasjonen ikke skal kunne endres eller slettes av uvedkommende (integritet) og at informasjonen ikke skal kunne leses av uvedkommende (konfidensialitet). De tre begrepene dekker sikringen av selve informasjonen.

Informasjonssystemene har sjelden verdi i seg selv, men det kan være hensiktsmessig å legge til beskyttelse av systemene som en del av sikkerhetsbegrepet. I et informasjonssystem er det mer enn bare informasjon som må vernes. Ressurser som for eksempel nettverkskapasitet, regnekapasitet og lagringskapasitet må også beskyttes. Videre består en vesentlig del av flere virksomheters produksjon av ren informasjonsbehandling. I slike tilfeller blir systemenes evne til å fungere til enhver tid et meget sentralt sikkerhetsaspekt, og sikring av selve informasjonen alene vil ikke være tilstrekkelig sett ut fra den aktuelle virksomhetens samlede behov. Dersom systemene svikter, vil det i tillegg til å medføre manglende oppfyllelse av virksomhetsmål, kunne svekke tilliten til at virksomhetene kan behandle informasjonen på sikker måte.

3 Gjennomføring av risikovurderinger

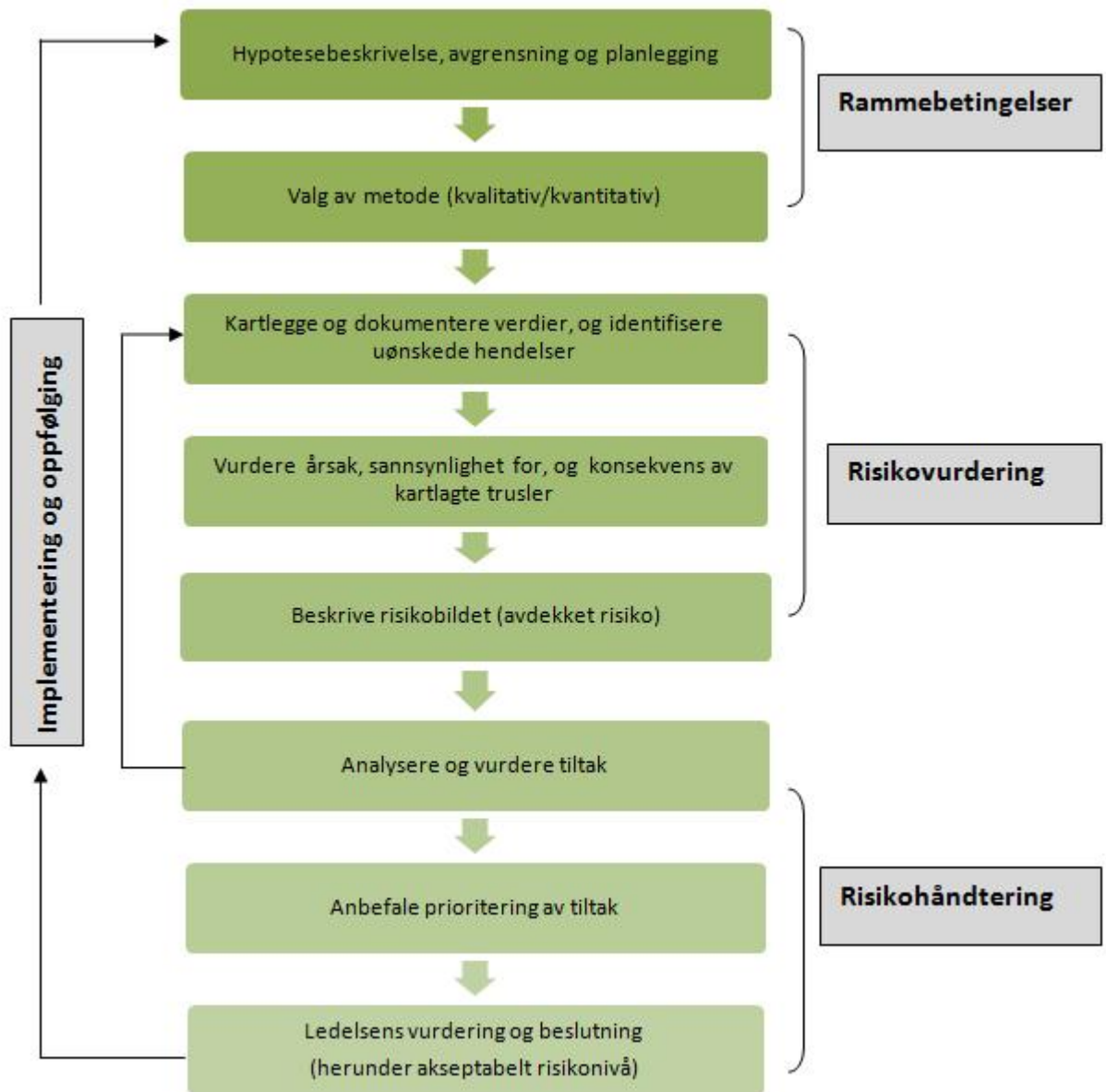
Risikovurderinger er et bidrag til:

- Å styre og holde risiko på et akseptabelt nivå
- Å kunne prioritere innsatsen på felter hvor den gjør mest nytte

Resultatet av en gjennomført risikovurdering er et innblikk i hvordan ”verden” ser ut på det tidspunkt risikovurderingen ble gjennomført, og er et grunnlag for å prioritere og velge riktige sikkerhetsforanstaltninger. Selve arbeidet er en prosess for å kartlegge og dokumentere et øyeblikksbilde av risiko forbundet med et gitt system.

Det kan ikke legges til grunn at tidligere utførte risikovurderinger for en type uønskede hendelser kan kopieres ukritisk fra en risikovurdering til en annen. Mulige uønskede hendelser vil være tett knyttet til hva som skal risikovurderes, aktuelle omgivelser og de tekniske forutsetningene er også i kontinuerlig endring. En tidligere utført risikovurdering vil imidlertid kunne være en god inspirasjonskilde for etterfølgende vurderinger, og for å finne frem til hvilke uønskede hendelser en ønsker å ta stilling til.

Kartleggingen av aktuelle og kommende trusler, deres angrepsveier og sannsynligheten for at truslene inntreffer, skal omsettes til hendelser som kan innplasseres i en konsekvensskala. Denne skala fastlegges sammen med ledelsen.



Risikovurderingenes kvalitet er avhengig av valgene og prioriteringene som gjøres gjennom hele prosessen. Resultatene, og argumentene bak disse, skal dokumenteres på en strukturert måte. En viktig del av oppgaven er også å kartlegge de verdier som må sikres og miljøet verdiene befinner seg i. Informasjonssikkerhetsarbeid er krevende. Ingen systemer er fullstendig sikre, det vil alltid være noe som kan gå galt.

Beskrivelsen av risikoen ved autentiserings-/ uavviselighetsmekanismen skal sammenholdes med det risikonivået som ledelsen har definert som akseptabelt. Når risikoen ved et nytt system vurderes, skal det også sammenholdes med den sikkerhetsrisiko som allerede eksisterer. Det er derfor også nødvendig å kartlegge eksisterende sikkerhetstiltak av både organisatorisk og teknisk karakter.

Risiko over det forhåndsdefinerte aksepterte nivået må håndteres ved hjelp av sikkerhetstiltak, enten for å redusere konsekvensene av, eller sannsynligheten for, uønskede hendelser (risikoreduserende tiltak).

Det forhåndsdefinerte nivået skal være dokumentert i virksomhetens styrende dokumentasjon for ivaretagelse av personvern og informasjonssikkerhet (internkontroll). Om en konkret risikovurdering viser at den aktuelle endringen ikke utfordrer den forhåndsdefinerte akseptable risiko, er det sjelden nødvendig å løfte saken, i seg selv, til ledelsen – kun der det er spørsmål om å velge å leve med en risiko utover det som opprinnelig er definert som akseptabel. Virksomhetens akseptable risikonivå skal ligge fast i forkant av prosessen, samtidig bør det forhåndsdefinerte nivået jevnlig vurderes i lys av nye risikovurderinger. Se for øvrig pkt. [3.2.6.1](#).

Risikovurdering av informasjonssystemer vil på mange områder skille seg fra øvrige risikovurderinger. Dette gjelder imidlertid ikke selve metodikken som benyttes, men hva som bør gjøres i de ulike stegene av prosessen. Selv om vurdering av risiko er helt sentral for informasjonssikkerhetsarbeidet, er det viktig å være bevisst på at risikovurdering, uansett hvilken metode som velges, ikke er en eksakt vitenskap.

Eksempler på spørsmål som bør besvares i en risikovurdering knyttet til autentiserings-/uavviselighetsmekanismen er:

- Hva skal forhindres?
 - at noen sender falsk søknad eller utgir seg for å være en annen?
 - at noen oppgir feilaktig informasjon?
 - id-forveksling/id-tyveri
 - feilaktig tildeling av rettighet eller ytelse?
 - at omsøkt prosess påbegynnes før tillatelse er gitt?
- Hva er sannsynligheten for at disse problemene inntreffer?
- Hvor stor skade vil hendelsene medføre?
- Vil det kunne bli rettssaker, for eksempel grunnet falske signaturer?

3.1 Forberedelsesfasen

- Arbeid med risikovurderinger gir best resultat hvis det organiseres som en tverrfaglig oppgave, og utnytter kompetanse innen flere fagfelt

I risikovurderingens forberedelsesfase er det viktig å avklare rammebetingelsene. Dette inkluderer beskrivelse av virksomhetens mål, hvilke deler av trusselbildet som skal undersøkes, andre avgrensninger, miljøet som skal vurderes og øvrige rammer for risikovurderingen. Målbeskrivelsen må omfatte hvem som berøres av arbeidet (virksomhet, avdeling, medarbeidere og eventuelt eksternt personell). Eventuelle avgrensninger vil typisk være relatert til omfang, spesielle forutsetninger eller antagelser, og resursbegrensninger knyttet til tid, bemanning, utstyr osv. Beskrivelsen av miljøet må omfatte den planlagte elektroniske tjenesten. Eierskap til alle objekter og prosesser på enheten må også være klart definert. Rammeverkets beskrivelse av risikonivåer bør da benyttes for å finne ut hvilket sikkerhetsnivå man antar tjenesten vil kreve. Se [kapittel 3.1.1](#) og [3.1.2](#) nedenfor.

Vanligvis vil problemene som identifiseres være knyttet til mer enn bare tekniske aspekter. Eventuell IT-sikkerhetskoordinator bør ikke utføre selve

arbeidet, men bistå med råd og veiledning i prosessen. Arbeidet skal utføres av personer som har den nødvendige faglige innsikt. Faglig innsikt innebærer at de kan vurdere de potensielle forretningsmessige konsekvensene av driftsmessig risiko ved informasjonsbehandlingen.

Et formål er å identifisere hendelser som kan få betydning for autentiserings-/uavviselighetsmekanismen ved tilkobling til åpne og lukkede nett, og av det kunne uttrykke en hypotese om konsekvenser av hendelsene og sannsynligheten for at de inntreffer. Både potensielle interne og eksterne uønskede hendelser må kartlegges.

Når rammebetingelsene er beskrevet, kan metode (se [kapittel 6](#) om metode) for den videre prosessen velges.

Omfang og detaljeringsgrad i planleggingen og organiseringen av arbeidet avhenger av sikkerhetsbehovet og virksomhetens størrelse/kompleksitet. En relativt enkel tilnæringsmetode vil ofte kunne gi gode resultater.

Risikovurdering kan utføres både i forkant og etterkant av en endring. En noe mer overordnet vurdering bør alltid foretas allerede i planleggingsfasen slik at de mest vesentlige områdene kan identifiseres så tidlig som mulig. Deretter bør det før endringen innføres, gjennomføres en noe mer detaljert undersøkelse for å sikre at de sentrale risikomomentene er håndtert. Dette for å kunne benytte de mest optimale og kostnadseffektive løsningene i beslutningsgrunnlaget for endringsprosessen.

Prosessens resultater, vurderinger og avveininger som er gjort skal kunne gjenbrukes.

Det er ingen fasit på hvordan virksomhetene skal gjennomføre denne type prosesser, og hvem som skal ha ansvar for hva. Plassering av ansvar til ulike roller i virksomheten er imidlertid sentralt. Det forekommer ulike benevnelser på stillinger, og i enkelte virksomheter er flere av oppgavene slått sammen. Et eksempel på fordeling av ansvarsroller kan være:

- Linjeledelsen sikrer at det gjennomføres risikovurderinger før det blir installert nye systemer
- Systemeiere/fagansvarlige har ansvar for å utarbeide en risikovurdering i henhold til egne krav
- Dataeiere har ansvar for å utarbeide risikovurdering i henhold til kravene for systemtilknyttede data. Dette skal skje i samarbeid med systemeieren
- Eiere av fysiske verdier (infrastruktur, komponenter, fasiliteter, operativsystemer og annen basissoftware) har ansvar for å utarbeide risikovurdering i henhold til kravene for disse verdiene
- Ansvarlige for informasjonssikkerhet beskriver rammene for arbeidet med risikovurdering som en del av virksomhetens informasjonssikkerhetsregime

3.1.1 Anbefalt prosess

Rammeverket legger opp til en prosess for risikovurdering der det innledningsvis bare vurderes konsekvenser av sikkerhetssvikt når det gjelder identitetskontroll (autentiseringen) eller bevissikring (uavviselighetsmekanismen). Formålet med vurderingen er å anslå løsningsens sikkerhetsbehov (risiko- og sikkerhetsnivå). Som et trinn to legger Rammeverket opp til at virksomheten gjennomfører en fullstendig risikovurdering, hvor både sannsynligheter for og konsekvenser av sikkerhetssvikt vurderes for den valgte løsningen.

I første trinn skal lite sannsynlige trusler utelates. Hvilke alvorlige konsekvenser som vil kunne oppstå dersom autentiseringsmekanismen svikter (herunder at uvedkommende får tilgang til opplysningene eller kan endre/slette informasjon), må imidlertid omfattes.

Resultatet av denne vurderingen kan sammenholdes med de fire risikonivåene som er definert i Rammeverket (se pkt 3.3 i [rammeverket](#)). Til hvert risikonivå hører et sikkerhetsnivå, slik at virksomheten på bakgrunn av valgt risikonivå kan se hvilke autentiserings- og uavviselighetsløsninger som passer.

3.2 Helhetlig risikovurdering

Mange problemstillinger vil fremstå som likeartede i arbeidet med å sikre løsninger for elektronisk kommunikasjon. Et typisk informasjonssystem vil være et distribuert system der flere brukere, ulike teknologier og arkitekturer inngår. I tillegg kommer forholdet til eksterne aktører, som underleverandører, outsourcingspartnere, konsulenter og forretningspartnere. Kontinuerlig endring og utvikling er også et viktig fellestrekk. Videre kan systemet som regel deles opp i en brukerdel og en driftsdel.

Når rammene for arbeidet er fastsatt, kan en mer helhetlig risikovurdering gjennomføres. Det vil da være naturlig også å vurdere krav til tilgjengelighet og andre sikkerhetsparametre som ligger utenfor Rammeverket. Å kartlegge verdier og identifisere uønskede hendelser er et naturlig utgangspunkt. Verdienes art og sikkerhetsbehov, og virksomhetens størrelse og kompleksitet er sentrale elementer.

3.2.1 Kartlegging av verdier

- Virksomheten bør tidlig kartlegge verdiene som vil bli berørt av en svikt i autentiserings- eller uaviselighetsmekanismen
- Begrepet verdi omfatter alle aktiva, både utstyr, programvare og informasjon

Verdier kan identifiseres ved å anslå taps- eller skadepotensial i form av kostnader ved gjenanskaffelse eller indirekte kostnader som tap av anseelse/tillit. Informasjon er et aktivum av verdi for virksomheten. Aktiva med lav verdi utelates.

Kartlegging må omfatte personopplysninger virksomheten har – antall, omfang og eventuelt beskrive behandlingen.

Personopplysninger kan i tillegg være av stor verdi for dem informasjonen gjelder. Dette kan være data som kanskje verken er virksomhetskritiske eller personfølsomme, men som kan oppleves som krenkende i hendene på uvedkommende.

3.2.1.1 Verdier på flere nivåer

For informasjonssystemer kan verdier finnes på flere nivåer:

- Sett mot informasjonssystemet – hvordan vil ulike hendelser i deler av systemet påvirke dets tilgjengelighet, integritet, konfidensialitet?
- Sett mot virksomheten – hvordan vil en svikt i informasjonssystemet påvirke virksomhetens mulighet til å gjennomføre sine oppgaver?
- Sett mot samfunnet – hvordan vil en svikt i informasjonssystemet kunne påvirke andre samfunnsfunksjoner, befolkningen osv.?

Kartleggingen må ta for seg grensene mellom miljøet som kartlegges og eksterne tilknytninger ("verden for øvrig"), samt grensene mellom forskjellige elementer internt i virksomheten. En slik form for miljøkartlegging må identifisere ulike grensesnitt, som koblinger mellom informasjonssystemet og eksterne datanett, fysiske yttergrenser, forholdet til kompetanse, rutiner, mv. (egeneksponering).

Ved vurdering av personvernrisiko representerer personopplysningene de verdiene som behandles. Potensialet for tap eller skade må knyttes til følgene for den enkeltes personvern. Personvern er vanskelig økonomisk målbart, og økonomisk gevinst ved misbruk er i mindre grad synlig som motivasjonsfaktor enn for eksempel ved industrispionasje.

I arbeidet med å anslå taps- eller skadepotensial er det naturlig å avdekke om informasjonssystemene inkluderer sensitive personopplysninger og/eller opplysninger som er underlagt taushetsplikt (hovedregel i [forvaltningsloven § 13](#)). Begrepet sensitive personopplysninger ([personopplysningsloven § 2 nr 8](#)) uttrykker et behov for konfidensialitet (behov for å holde opplysningene skjult for uvedkommende). Tilsvarende gjelder opplysninger underlagt taushetsplikt.

Taps- eller skadepotensialet kan ikke knyttes til opplysningstypen alene. Også formålet med behandlingen og omfanget av personopplysninger påvirker sikkerhetsbehovet. Eksempelvis vil manglende konfidensialitet for pasientopplysninger benyttet for statistikk medføre tap av anseelse og personlig integritet. Manglende tilgjengelighet for de samme opplysningene benyttet for medisinsk behandling, vil kunne få følger for liv og helse. (Eksempelet er hentet fra Datatilsynets veileder)

Informasjonsverdier kan i hovedsak påvirkes av tre typer uønskede hendelser:

- Utlevering
- Utilgjengelighet
- Endring

Hendelsene kan detaljeres ytterligere:

- Utlevering - kan informasjonen tilbakeføres eller er skaden permanent?
- Utilgjengelighet - for et avgrenset tidsrom eller permanent?
- Endring - sporbar og kan rettes, sporbar og permanent, ikke sporbar?

3.2.1.2 Tilgjengelighet

Når det gjelder verdien av tilgjengelighet er det naturlig å ta utgangspunkt i de funksjoner som verdiene understøtter (f.eks. inndrivelse av skatt, svar på forespørsler fra enkeltpersoner, utbetaling av ytelser, rapportering). Konsekvensen av brudd vil være avhengig av det tidsrom hvor tilgjengelighet mangler, eller hvor hyppige bruddene er. Hyppige, kortvarige avbrytelser som skyldes ustabil drift kan være problematiske. Det kan derfor være nødvendig å definere en tidsakse, hvor det angis kritiske terskler som svarer til hvert konsekvensnivå.

- Opplysninger om hvor verdiene er plassert (kan inntegnes i plan- og arkitekturtegninger)
- Blir verdiene flyttet eller overført? (fra, til, hvordan, når?)
- Hvordan oppbevarer virksomheten verdiene?
- Ekstern eller intern opprinnelse?
- Rutiner for destruksjon av verdiene?
- Hvem administrerer/vedlikeholder - og hvordan?
- Andre opplysninger om bruksmønsteret

3.2.1.3 Omfang og detaljeringsgrad

Å definere omfang og detaljeringsgrad for kartleggingen kan være vanskelig. Arbeidet må tilpasses forholdene i virksomheten. Risikobildet vil være avhengig av flere faktorer, som for eksempel av kompleksitet/uoversiktighet (antallet lokasjoner, informasjonssystemets kompleksitet osv.) og risikobildet i omgivelsene. Generelt vil behovet for dokumentasjon og styring stige proporsjonalt med disse faktorene.

Kartlegging av verdier skal resultere i en oversikt hvor antatt sikkerhetsbehov knyttes til den enkelte verdi. Anslått taps- eller skadepotensial gir grunnlag for antagelser om sikkerhetsbehovet.

Det er vanlig å kategorisere virksomhetens verdier i tre klasser, og vurdere tap ved uønskede hendelser opp mot disse:

- Økonomi: tapt eller forsinket produksjon, skade på utstyr og eiendom, svindel, tyveri, erstatningsansvar, tapt arbeidstid
- Tillit og anseelse: tillit hos publikum, marked, samfunn, ansatte og eventuelt regulerende organ (offentlige tilsyn, konsesjonsutstedere o.l.)
Kan også ses på som langsiktige økonomiske verdier
- Helse, miljø og sikkerhet (HMS): Tap av liv og personskade, samt skade på miljø og omgivelser

For offentlig sektor ligger det også en betydelig verdi i trygg og korrekt saksbehandling, en verdi det også kan være hensiktsmessig å vurdere.

3.2.2 Identifisere uønskede hendelser

Spørsmål til hjelp for å identifisere hendelser:

- Hva kan skje?
- Hvor kan det skje?
- Hvem er involvert?

Hver hendelse kan utdypes:

- Hva er de positive og negative konsekvensene av hendelsen?
- Kan det settes en verdi på konsekvensen?
- Hvor sannsynlig er det at hendelsen vil finne sted?
- Hvilke faktorer har innflytelse på konsekvenser og sannsynligheter?
- Hvilke kontrollmekanismer er satt i verk for å begrense risikoen for hendelsen?

Uønskede hendelser identifiseres ved å kartlegge trusler systemet er utsatt for og sårbarheter systemet innehar.

Dette kan det være hensiktsmessig å gjøre i forkant av selve risikovurderingen (og kvalitetssikre i løpet av selve prosessen). Formålet med dette er å få en oversikt over trusselbildet.

En uønsket hendelse i autentiserings-/ uavviselighetsmekanismen er handling eller tilstand med utilfredsstillende sikring av personopplysninger og/eller når informasjon og objekter blir kompromittert. Med kompromittering av informasjon menes tap av konfidensialitet, integritet og tilgjengelighet.

Trusler må vurderes og mulige hendelser som kan føre til sikkerhetsbrudd må identifiseres. Utvelgelsen må ta utgangspunkt i det taps- eller skadepotensial som er anslått ved kartlegging av verdier og miljø. Det er en utfordring i å

begrense vurderingen til det som er relevant, uten å inkludere så mye at prosessen ikke kan gjennomføres innen rimelig tid. For å unngå å bruke for mye tid på fareidentifikasjonen kan sjekklister være nyttige som hjelpemiddel (Se eksempler etter DS484.³)

Det kan være hensiktsmessig å skille mellom tilsiktede og ikke-tilsiktede uønskede hendelser.

I noen tilfeller vil potensielle lekkasjer være begrenset til relativt små mengder personopplysninger. Imidlertid vil gjentatte lekkasjer med små mengder opplysninger, samlet sett, kunne danne en mer detaljert profil av enkeltindivider. Også informasjon som i utgangspunktet fremstår som anonym kan i tilstrekkelig kvantum, utilsiktet, identifisere enkeltindivider.

Kompromittering kan, noe forenklet, skje på tre måter:

- Eksterne trusselaktører – aktører som gjennom bevisste handlinger prøver å få innsyn i informasjon, alternativt manipulere eller gjøre den utilgjengelig.
- Egeneksponering – økt sårbarhet ved at egenesikring ikke fungerer tilfredsstillende (kan utløses gjennom bevisste og ubevisste handlinger).
- Utro tjenere – egne ansatte som bevisst bidrar til at informasjon kompromitteres. (Drivkreftene kan være egen vinning eller press fra eksterne aktører.)

Noen tiltak, som for eksempel redundans (overskuddsinformasjon/samme informasjon som blir lagret flere ganger, gjerne på ulike måter) programvareoppdateringer, viruskontroll, nødstrøm og så videre kan enkelt knyttes til relevante uønskede hendelser, mens andre, som for eksempel overvåking, dokumentasjon, oversiktighet, varslingsrutiner, generell sikkerhetskultur osv. er mer generelt.

I den grad det legges opp til å benytte felleskomponenter, må den ansvarlige virksomhet redegjøre for sikkerheten i løsningen – herunder hvilke trusler den skal er ment å takle.

Det er viktig å være klar over at Rammeverket ikke berører sårbarheter i it-infrastrukturen hos bruker, herunder brukers datautstyr og hans sikkerhetskompetanse. Virksomheten må derfor vurdere dette, eksempelvis risikoen for at det forekommer ondsinnet programvare hos brukeren uten at vedkommende kjenner til det, eller at brukeren forledes til å kommunisere med "falske" nettsteder.

³ <http://www.itst.dk/it-sikkerhed/ds-484>

Noen hendelser som kan lede til uheldige konsekvenser:

- Uautorisert endring av personinformasjon
- Sensitive personopplysninger gjøres kjent for uvedkommende
- Omsetningstall lekker ut før kvartalsrapportering
- Feil i utbetalingsgrunnlag av trygd
- Feil i utbetalingsgrunnlag for MVA
- Uautorisert endring for å påvirke offentlige utbetalinger
- Tap av renommé etter medieoppslag om datainnbrudd
- Bevismateriale blir ødelagt eller kommer på avveie, på grunn av operatørfeil
- Uautorisert endring av personadresse som ledd i identitetstyveri

3.2.3 Årsak

I en årsaksvurdering er formålet å kartlegge de mulige hendelsesforløpene som kan forårsake en hendelse. Årsaken er den aktivitet eller situasjon som får den uønskede hendelsen til å inntreffe. Årsaker til at uønskede hendelser utløses er ikke nødvendigvis direkte handlinger fra personer. Påvirkning fra omkringliggende miljø, herunder varme (brann/overtemperatur), vann (oversvømmelse/fukt), smitte fra hendelser i nærliggende virksomheter er like aktuelle.

For å sikre at alle hendelser av betydning avdekkes og omfattes, bør hendelser og årsaker beskrives hver for seg. Dette vil også kunne bidra til at viktige årsaker blir mer synlige og dermed være til bedre hjelp ved valg av sikkerhetstiltak. Manglende skille mellom hendelser og årsaker vil kunne resultere i beskrivelser som tilsynelatende dekker en rekke hendelser, men som i realiteten kun beskriver én hendelse med flere mulige årsaker.

Uønskede hendelser kan følge av både eksterne og interne forhold. Dårlige holdninger og rutiner, menneskelig feil, slurv og manglende sikkerhetstiltak øker sannsynligheten for at eksterne trusselaktører kan lykkes med angrep. Eksterne trusselaktører vil gjerne lete etter sikkerhetsmangler for å nå sitt mål. I tillegg kan det også være personer innenfor virksomheten (utro tjenere) som bevisst forsøker å volde skade eller kompromittere for eksempel sensitiv informasjon.

Erfaringsmessig skjer de fleste uønskede hendelser i et informasjonssystem uten overlegg. Slike hendelser kan grovt deles i tre kategorier:

- Menneskelige feil. Feil som oppstår i forbindelse med systemdesign, arkitektur, implementering, bruk, drift, overvåking og vedlikehold. Mange av disse vil være menneskelige feil gjort utenfor systemeiers kontroll – for eksempel problem forbundet med ustabil programvare.
- Fysisk svikt. Dette inkluderer for eksempel fysisk slitasje (harddisker o.l.), kabelbrudd, kontaktfeil og komponentfeil som følge av varmeutvikling. Ofte vil de bakenforliggende årsakene igjen være menneskelige feil, som for eksempel feil dimensjonering, manglende utskifting av gammelt utstyr eller mangelfull overvåking.

-
- Miljø/naturhendelser. Oversvømmelse, vannskader, brann, lynnedslag og vind.

Med tilsiktede uønskede hendelser menes angrep på, eller manipulasjon av, informasjonssystem og tilhørende infrastruktur. Dette omfatter fysiske angrep og ødeleggelser, samt logisk og sosial manipulasjon av system og virksomhet. De siste årene har en også sett en økning i denne type hendelser, og en utvikling der økonomisk gevinst stadig oftere er målet. Dette kan involvere alt fra utsendelse av uønsket e-post eller fremvising av reklame, til for eksempel direkte angrep på økonomisk infrastruktur. Mesteparten av de tilsiktede hendelsene i et informasjonssystem oppstår på grunn av massedistribuert ondsinnet kode (virus) som ikke er rettet mot spesifikke virksomheter.

Målet er å beskrive årsaker (og hendelser) detaljert nok til at konsekvens- og sannsynlighetsvurdering kan gjennomføres og være til hjelp i arbeidet med valg av sikkerhetstiltak. Nødvendige sikkerhetstiltak vil i mange tilfeller kunne angis allerede på grunnlag av årsaksvurderingen.

3.2.4 Sannsynlighet og konsekvens

For hver hendelse som er identifisert må sannsynligheten for at den vil inntreffe og eventuell konsekvens av dette vurderes. I risikobegrepet ligger det en hypotese om sannsynlighet for at en uønsket hendelse skal inntreffe. For å kunne uttrykke noe kvalifisert om risiko i denne relasjonen, er det nødvendig å sette et mål på sannsynligheten for, og konsekvensen av, den uønskede hendelsen.

Sannsynlighet er i Rammeverket (se pkt. 3.1 s 9) beskrevet ved hjelp av begrepene frekvens (hvor ofte en sårbarhet historisk blir forsøkt utnyttet) og kapasitet (en uautoriserets evne til å utnytte en sårbarhet, hvor vanskelig det er å utnytte sårbarheten og hvor lett det er å skalere/øke omfanget av et angrep). Motivasjon/vinning (hvor interessant er det å utnytte en sårbarhet) inngår også som et element.

Alle konsekvenser har sin bakgrunn i en eller flere hendelser som oppstår med en viss sannsynlighet. For noen hendelser foreligger god statistikk, slik at det er noenlunde enkelt å angi frekvens. Andre hendelser må større grad baseres kvalifisert gjetting på for å finne sannsynlighet.

Konsekvens er beskrevet (se Rammeverket pkt. 3.2 s 10) som resultatet av at en sårbarhet blir utnyttet eller en uheldig hendelse inntreffer, uavhengig av sannsynligheten for at det skal skje. Det kan, som tidligere nevnt, uttrykkes i økonomisk tap, men også relateres til virksomhetens anseelse og eventuelt straffeansvar for virksomhet og ledelse. Konsekvens skal vurderes for alle parter, brukere av tjenesten (privatpersoner og næringsliv), virksomheten selv og offentlig sektor som helhet. Formålet ved vurdering av personvernrisiko er noe ulikt, men det inngår som et naturlig element i arbeidet med å avdekke øvrig risiko ved virksomheten. Selve metoden for vurdering av konsekvens, og for risikovurderingen for øvrig, er den samme.

Ved å angi sannsynlighet og konsekvens som en kvantitativ størrelse, kan en synliggjøre og oppsummere resultater fra risikovurdering. Dette kan videre benyttes ved sammenligning av vurderinger fra ulike hendelser. Kvantitativ beskrivelse vil også være til hjelp i arbeidet med å avdekke restrisiko.

Kombinasjonen av sannsynlighet og konsekvens kan settes inn i en matrise (eller multipliseres) for å angi et risikonivå. Risikonivået sier noe om hvilket nivå det bør være på sikkerhetstiltakene (se [kapittel 4](#)). For å gi best mulig grunnlag for de videre vurderingene anbefales at sannsynlighet og konsekvens angis kvantitativt med flere verdier i en 4x4 eller 5x5-matrise. Dette skal gjøres for hver hendelse. Det ligger imidlertid en utfordring i forhold til å finne fornuftig gruppering – fordeling av hendelser.

Risikonivåene bør deretter tilordnes ulike kombinasjoner av sannsynlighet og konsekvenser, eksempelvis slik:

K4				R4
K3			R3	
K2		R2		
K1	R1			
Konsekvens (K)/ Sannsynlighet (S)	S1	S2	S3	S4

- Eksempel: Brudd på lov/forskrift alltid registreres som K4.

Hendelser med lav konsekvens og høy sannsynlighet viser seg ofte å være enkelt å innta i en risikovurdering. Hendelser med høy konsekvens og lav sannsynlighet er mer komplisert. En hendelse med hyppighet 10 ganger i året som utløser en konsekvens med kostnad 15 000 hver gang gir en risiko som koster 150 000 i året. En hendelse som antas å inntreffe hvert 20. år, men som påfører enheten en kostnad på 3 000 000 om den skulle skje, gir også en risiko med statistisk kostnad 150 000 i året. Det er viktig at denne type trusler ikke utelates fra vurderingene.

Flere kombinasjoner av konsekvens og sannsynlighet kan gi tilsvarende risikonivå (liten konsekvens, høy sannsynlighet – stor konsekvens, lav sannsynlighet). Hensikten med å fastsette risiko er å få oversikt over trusselbildet, og bruke dette som grunnlag for å redusere de risikoer som ikke kan aksepteres. Det er også et viktig verktøy for å prioritere riktig (kost/nytte perspektiv), for ikke å bruke ressurser på forhold som er uvesentlig.

Risiko uttrykt som produkt av to størrelser gjør det enklere å sammenligne avdekket risiko med det akseptable risikonivå som er besluttet.

3.2.4.1 Nærmere om sannsynlighet

3.2.4.1.1 Statistisk metode

Det er flere måter å vurdere sannsynlighet for at en uønsket hendelse vil kunne inntreffe. I den grad historiske (statistiske) data om identiske eller tilsvarende hendelser eksisterer, vil en sannsynlighetsvurdering kunne ta utgangspunkt i dette. Vurdering av sannsynlighet vil da kunne baseres på statistiske metoder, og svaret kan angis kvantitativt.

Vurdering av sårbarhet skal gi et overblikk over hvor godt virksomheten er beskyttet mot hendelser gjennom de sikringsforanstaltninger som virksomheten allerede har. Det vil si sannsynligheten for at en hendelse inntreffer med de eksisterende sikringsforanstaltninger.

Kvantitativ angivelse av sannsynlighetsgrad kan oppgis slik ([Datatilsynets veiledning](#)⁴ s. 15):

- S=4; Svært sannsynlig (hendelsen inntreffer flere ganger hvert år)
- S=3; Meget sannsynlig (hendelsen inntreffer årlig eller sjeldnere)
- S=2; Sannsynlig (hendelsen inntreffer en gang pr 10 år eller sjeldnere)
- S=1; Lite sannsynlig (hendelsen inntreffer en gang per 50 år eller sjeldnere)

Historiske data er ikke alltid beskrivende for systemet som skal vurderes. Relatert til autentiserings-/ uavviselighetsmekanismen vil risikovurdering gjerne gjennomføres for nye verdier og/eller nytt miljø, og historiske data er derfor ikke tilgjengelige. For øvrig foregår utviklingen av programvare, maskinvare og arkitekturløsinger så raskt at det relativt sjelden foreligger relevant statistisk materiale. For rent tekniske enkelthendelser, som harddiskhavari og strømbrudd, kan det foreligge gyldig statistikk. Hendelser som ønskes analysert er gjerne mer komplekse, med flere barrierer og sårbarheter, som må vurderes samtidig.

3.2.4.1.2 "Letthetsvurdering"

Mangler historiske data kan en såkalt "letthetsvurdering" være et alternativ. "Letthetsvurderinger" skal avdekke sårbarhet, hva som skal til for at en hendelse kan inntreffe. Vurderingen må beskrive behovet for resurser i form av utstyr og programvare, og i form av kompetanse og evner. Hvor mye som skal til av tilfeldigheter, kvalifisert kunnskap og grad av besluttsomhet -vil uaktsomhet, forsett eller overlegg være tilstrekkelig? Trusler kan også komme fra omgivelsene, der ikke mennesker nødvendigvis er direkte involvert. Mulighet til å forårsake hendelsen, utforming av miljøet, herunder

⁴ Se: http://www.datatilsynet.no/templates/article____888.aspx

organisatoriske og tekniske sikkerhetstiltak må inngå som en del av utgangspunktet.

Motivasjon kan være knyttet til følelser som rettferdighet, prestisje, hevn og ødeleggelseslyst. Dette kan være vanskelig å avdekke. Et alternativ er å anslå innsatsen som må til for å forårsake hendelsen. Begrepene uaktsomhet, forsett og overlegg kan benyttes for å angi denne innsatsen. Et utgangspunkt for vurderingen kan være en beskrivelse av miljøet. Verdienes art kan også påvirke motivasjonen. Vurderingen må avdekke om noen kan ha nytte av å utføre en hendelse, og i så fall hvem (interne/eksterne). Når målet er økonomisk gevinst for den som forårsaker hendelsen, kan spørsmålet konkretiseres til hvordan andre kan nyttegjøre seg verdiene. Nytte i denne sammenheng kan eksempelvis være betaling for utlevering av opplysninger eller etter trusler påvirke ved å hindre tilgang til, eller skade/endre opplysninger. Anslag for andres mulige gevinst, i tillegg til taps- og skadepotensial for virksomheten selv, er derfor et naturlig element.

For felleisløsninger vil det foreligge en analyse av sårbarhet (letthetsvurdering) og eventuelt også erfaringstall. Det er en forutsetning at tjenesteeier er kjent med innholdet i dette før tilkobling og at det inngår som et element i risikovurderingen.

Datatilsynet har i [sin veiledning](#) foreslått følgende skala for sannsynlighet gradert etter letthet:

S=4, sikkerhetstiltak er ikke etablert, eller kan omgås/brytes av egne medarbeidere og eksternt personell med små til normale ressurser. Det er ikke nødvendig med kjennskap til tiltakene. Sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående.

S=3, sikkerhetstiltak er ikke fullt etablert, eller fungerer ikke etter hensikten. Egne medarbeidere trenger kun små til normale ressurser for å omgå/bryte tiltakene, det er ikke nødvendig med kjennskap til tiltakene. Eksternt personell trenger normal kjennskap til tiltakene (eksempelvis til hvilke rutiner som gjelder, eller hvordan sikkerhetsteknologi er implementert), i tillegg til små/normale ressurser. Inngrep forutsetter forsett (bevisst eller aktivt) for å bryte sikkerhetstiltakene.

S=2, sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten. Tiltakene kan likevel omgås/brytes av egne medarbeidere med små til normale ressurser, som i tillegg har normal kjennskap til tiltakene. Eksternt personell trenger gode ressurser, og god/fullstendig kjennskap til tiltakene for å omgå/bryte disse. Utenforstående må opptre med overlegg og ha noe kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.

S=1, sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten. Tiltakene kan kun omgås/brytes av egne medarbeidere med gode ressurser, og god/fullstendig kjennskap til tiltakene. Eksternt personell kan ikke

omgå/bryte tiltakene. 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.

3.2.4.2 Nærmere om konsekvens

- Virksomheten konsekvensvurderer i første omgang hendelsene kvalitativt ved bruk av passende skala (f. eks. lite farlig - farlig - kritisk - katastrofalt)
- Skalaen bestemmer om en verdi anses som kritisk. Hvor "snittet" legges er virksomhetens egen beslutning. Det kan velges flere strategier, f.eks. å anse alt i øverste del av skalaen som kritisk. Deretter utarbeide en kost-nytte-betraktning (kvantitativ vurdering) for verdier på det nest høyeste trinnet
- Hvor "finmasket" skalaen bør være, vil variere fra virksomhet til virksomhet

Konsekvens er, som tidligere nevnt, resultat av at en sårbarhet blir utnyttet eller en uheldig hendelse inntreffer, uavhengig av sannsynligheten for at det skal skje. Konsekvens vil i første rekke være knyttet til verdienes art. I tillegg vil det være av betydning hvor mange personer som berøres. Personvernkonsekvens må rangeres høyere dersom hendelsen får følger for mange mennesker. Dette selv om følgene for den enkeltes personvern vurderes som liten.

Konsekvens må vurderes for alle parter, brukere av tjenesten (privatpersoner og næringsliv), den offentlige virksomheten selv og offentlig sektor som helhet. I kompliserte systemer med autentiserings-/ uavviselighetsmekanismer kan det være vanskelig å forutsi hvilke konsekvenser som kan inntreffe. I systemer som er tett sammenkoblet, kan en hendelse utløse en annen hendelse som i utgangspunktet ikke var forutsett. Det er derfor viktig å holde alle muligheter åpne i arbeidet med å identifisere uønskede hendelser.

Som regel vil det være mest interessant å avdekke konsekvenskjeder eller årsakssammenhenger bak konsekvensene som kan inntreffe. Det kan derfor være nyttig å angi konsekvensene detaljert, for eksempel "nedetid", "feil i datagrunnlag", i motsetning til "mangel på tilgjengelighet" og "brudd på integritet". Ved å detaljere konsekvensene/årsakssammenhenger vil det være enklere å treffe sikkerhetstiltak som faktisk vil avhjelpe, eller redusere sannsynligheten for at nettopp denne konsekvensen inntreffer.

Tap av tillit til offentlige virksomheters behandling av personopplysninger trenger ikke ha grunnlag i reelle lekkasjer eller tap av data, men kan like gjerne følge av enkeltmenneskenes forestilling av hvilken risiko deres personlige informasjon utsettes for.

Også konsekvens for autentiserings-/ uavviselighetsmekanismen må angis som en kvalitativ beskrivelse og kvantitativ størrelse.

Datatilsynet [foreslår følgende skala](#) for konsekvensgradering:

- K=4; Katastrofalt
- K=3; Kritisk
- K=2; Farlig
- K=1; Lite farlig

I vurderingen er det naturlig å ta utgangspunkt i beskyttelse av liv/helse, økonomi og anseelse/personlig integritet for enkeltmennesker. Det bør også tas hensyn til eiendeler/objekter som påvirkes, mulighet for erstatning, eventuelle reserverløsninger og eksisterende tiltak.

Nivåene kan defineres slik:

- K=4, hendelsen kan føre til tap av liv eller vedvarende helsetap, eller kan medføre betydelig og uopprettelig økonomisk tap, eller kan føre til alvorlig tap av anseelse eller integritet som påvirker liv, helse eller økonomi.
- K=3, hendelsen kan føre til tap av helse, eller kan medføre uopprettelig økonomisk tap, eller kan føre til alvorlig tap av anseelse og integritet.
- K=2, hendelsen kan medføre betydelig økonomisk tap som kan gjenopprettes, eller kan føre til tap av anseelse eller integritet (eksempelvis kompromittering av opplysninger den registrerte oppfatter som krenkende, eller som andre kan gjøre nytte av).
- K=1, hendelsen kan medføre økonomisk tap som kan gjenopprettes, eller kan føre til tap av anseelse eller integritet (eksempelvis kompromittering av opplysninger den registrerte oppfatter som følsomme).

3.2.5 Beskrive avdekket risiko

Det er en utfordring for sikkerhetsarbeidet å rette fokus mot alle relevante trusler, både eksterne og interne. Risikovurdering skal resultere i en rangert oversikt over relevante uønskede hendelser, eventuelt en matrise som illustrerer sannsynlighet for og konsekvens av de ulike hendelsene. En slik oversikt samsvarer ikke nødvendigvis med prioriteringsrekkefølgen for relevante tiltak.

3.2.6 Analysere og vurdere tiltak

Når risikobildet er beskrevet, må risikoen analyseres og tiltak vurderes. Virksomheten skal vurdere, og tydeliggjøre, om avdekket risiko er innenfor området for akseptabel risiko -slik ledelsen har definert det på forhånd. Det samme gjelder i forbindelse med hendelser som representerer brudd på regelverk, enten dette er lovkrav, inngåtte avtaler eller virksomhetens egne retningslinjer. Arbeidet omfatter også å fremstille den ledelsesinformasjon som skal danne grunnlag for at ledelsen kan beslutte strategi og handlingsplaner.

Vurderte hendelser og de relevante tiltakene opptrer sjelden uavhengig av hverandre.

3.2.6.1 Akseptert risikonivå -ledelsesbeslutning

- Virksomhetens risikovillighet er det ledelsen som må angi
- Tilsynsmyndighetene har kompetanse til å fastlegge kriterier for akseptabel risiko. Det skal imidlertid mye til før valg anses som "feil" så lenge de kan begrunnes og forsvares i ettertid

For å kunne utøve forsvarlig risikostyring er det nødvendig med noen nedfelte kriterier. Dette omfatter holdepunkter for å kunne angi når en risiko øker eller er på et nivå ut over det som på forhånd er akseptert. Hvilke konsekvenser risikovurderingen skal ha må relateres til ledelsens beslutning om hvilket risikonivå som ut fra en helhetsbetraktning er akseptabelt for virksomheten.

Beskrivelse av akseptert risikonivå skal inngå som et element i grunnlaget for risikovurdering, og inngår på den måte som et naturlig element i både første og siste fase i risikovurderingen.

Ansvar for å beslutte hva som er akseptert risikonivå ligger hos virksomhetens ledelse. Akseptkriteriene vil imidlertid også påvirkes av ytre rammevilkår og lovpålagte krav. Det vil normalt forekomme et antall trusler hvor vurdering av risikonivået ligger på "farlig" eller over. Trusler innenfor risikonivåområdene "kritisk" og "katastrofal" vil man typisk skulle gjøre noe ved umiddelbart.

Akseptert risikonivå skal relateres til både konfidensialitet, tilgjengelighet og integritet. I noen situasjoner kan de tre kriteriene komme i konflikt, for eksempel kan for vid tilgang til helseopplysninger innebære krenkelse av taushetsplikt, mens for streng tilgangsstyring vil kunne svekke muligheten til forsvarlig helsehjelp. Det er derfor viktig at kryssende hensyn identifiseres og at prioritering mellom forskjellige behov synliggjøres. Særlig vil behov for konfidensialitet og tilgjengelighet kunne være vanskelig å forene.

Beskrivelsen av akseptert risikonivå for autentiserings-/ uavviselighetsmekanismen må være relativt detaljert og konkret. Beskrivelsen bør angi hendelser med betydning for mekanismene, hvilke personopplysninger og behandlinger av personopplysninger, som berøres. Videre må den inneholde prioritering mellom forskjellige sikkerhetsbehov, og på overordnet nivå beskrive risikoreducerende tiltak.

Beslutning om akseptabelt risikonivå for virksomheten som helhet skal blant annet komme til uttrykk i virksomhetens sikkerhetsmål. Vurderingene knyttet til autentiserings-/ uavviselighetsmekanismen bør inngå i dette helhetlige målet. Sikkerhetsmålet skal, på et overordnet nivå, beskrive formålet med bruken av informasjonsteknologi og angi sikkerhetsbehov. Beskrivelse av akseptabelt risikonivå for autentiserings-/ uavviselighetsmekanismen kan også inngå i instruks for informasjonssikkerhet, som del av informasjon om forventet sikkerhetsnivå.

3.2.6.2 Ansvar for valg av sikkerhetsnivå

Hver offentlig virksomhet er selv ansvarlig for å forvalte sine oppgaver på en forsvarlig måte. Virksomheten må selv vurdere hva som er et akseptabelt risikonivå og hvilke sikkerhetsløsninger som sikrer tjenestene forholdsmessig akseptabelt. Rammeverkets anbefalinger om hvilket sikkerhetsnivå som egner seg for de definerte risikonivåer fritar ikke virksomheten fra ansvar eller krav til selv å vurdere sikkerhetsbehovet i forhold til konkrete tjenester som (skal) tilbys. For personopplysninger er virksomheten ansett som behandlingsansvarlig etter personopplysningsloven.

På bakgrunn av risikovurdering skal virksomheten kunne vurdere hvilket risikonivå som passer den aktuelle type elektronisk kommunikasjon. Rammeverket gir følgende anbefaling om hvilke sikkerhetsnivåer som egner seg for de forskjellige risikonivåer:

- Risikonivå 1 - Sikkerhetsnivå 1
- Risikonivå 2 - Sikkerhetsnivå 2
- Risikonivå 3 - Sikkerhetsnivå 3
- Risikonivå 4 - Sikkerhetsnivå 4

Rammeverket og denne veiledningen er generelle verktøy for offentlige virksomheter. Verktøyet skal være egnet for å tilpasse tjenester eller samhandling etter sikkerhetsnivå og til påfølgende valg av løsning for autentisering eller uavviselighet. Det kan også brukes til å velge sikkerhetsnivå eller sikkerhetsløsning for offentlige løsninger (portaler) der en autentisering kan gi adgang til flere tjenester. Videre er det anvendelig for å vurdere gjenbruk av andres sikkerhetsløsninger eller felles sikkerhetsløsninger mot egne tjenester.

4 Anbefalte tiltak

Ved vurdering av sikkerhetstiltak er det også nødvendig å ta hensyn til:

- Kriterier for kvalitet, funksjon og konsistens
- Om tiltakene er fullstendige og dekkende?
- Gjennomførbarhet (praktisk og kostnadmessig)
- Om tiltakene gir ønsket effekt (verifikasjon)

Risikohåndtering skal iverksettes når risikovurderingen viser at risikonivået er høyere enn det akseptable. Valg av sikkerhetstiltak er ikke en del av risikovurderingen, men anbefaling av tiltak bør være en del av vurderingen. Risikomatriksen ([hyperlink](#)) viser hvilke uønskede hendelser som representerer den største risiko.

Sikringstiltak har normalt en kostnad, både ved implementering og drift. Det er derfor ikke sikkert at det alltid er ønskelig eller fornuftig å sette inn sikringstiltak utover det som må til for å redusere risikoen på et akseptabelt nivå. Enkelte tiltak kan ha så lave kostnader at det gjennomføres til tross for lav risiko, mens andre tiltak kan være så kostbare at de i realiteten ikke lar seg gjennomføre. Videre kan noen tiltak for eksempel fjerne flere risikoer, og en kostnytteanalyse av de relevante tiltakene er derfor et naturlig og ofte et nødvendig tiltak.

De færreste investeringer i forebyggende sikkerhet genererer nytte i form av inntekter. En alternativ måte å vurdere nytte vil heller være å se på nytte som unngåtte utgifter. Utover dette må nytte begrunnes kvalitativt.

4.1 Preventive og reaktive tiltak

Tiltak deles tradisjonelt inn i to kategorier, preventive og reaktive. Preventive tiltak skal redusere sannsynligheten for at en hendelse inntreffer, mens de reaktive skal redusere konsekvensen når hendelsen har inntruffet. Eksempler på tiltak er sikkerhetskopiering, kryptering og brannmur.

4.2 Risikostyring - suksesskriterier

Suksesskriterier:

- Ledelsen ser på risikostyring som et viktig og nødvendig verktøy
- Representanter for ulike deler av virksomheten er involvert i arbeidet
- Utføringen gjøres så enkelt som mulig
- Prosessen har tilstrekkelige ressurser og nødvendig kompetanse. (om kompetansen finnes internt i virksomheten eller om det bør leies inn eksterne er avhengig av den enkelte virksomhet.)
- Resultatene følges opp
- Risikovurderinger er en naturlig del av virksomhetens beslutningsprosesser
- Risikovurderingene og tilhørende dokumentasjon oppfyller lov- og forskriftskrav

Vurderinger av økonomisk nytte vil gjennomgående måtte fremlegges i forbindelse med anbefaling av investeringsutgifter. I mange tilfeller er det imidlertid vanskelig å fastsette økonomisk nytte ved de tiltakene som ønskes implementert, samtidig som de færreste investeringer i forebyggende sikkerhet genererer nytte i form av inntekter. Et alternativ kan være å vurdere nytte i form av unngåtte utgifter, eventuelle kostnader ved et sikkerhetsbrudd. Utover dette må nytte begrunnes kvalitativt.

De aller fleste sikringstiltak har en kostnad, både ved implementering og drift. Kostnadseffektivitet skal være et element i vurderingen av nye tiltak. Det er ikke nødvendigvis slik at høyest mulig sikkerhet alltid er ønskelig eller fornuftig. Investeringskostnadene for sikringstiltak må veies mot det potensielle tapet som et sikkerhetsbrudd kan forårsake.

5 Revisjon og kontroll

- Korrekt håndtering av avvik skal bidra til god risikostyring og effektiv gjennomføring
- Kritiske situasjoner skal håndteres med minst mulige skadevirkninger

I utgangspunktet er ikke dette trinnet en naturlig del av risikovurderingen, men en viktig del av virksomhetens risikohåndtering. Risikohåndtering er ikke en enkeltstående aktivitet, men en kontinuerlig prosess. Dette betyr at risikobildet må overvåkes og vurderes kontinuerlig. Oppfølging og kontroll av sikkerhetsarbeidet, samt ledelsens evaluering av sikkerhetstilstanden, vil uansett være et nyttig underlag for fremtidige risikovurderinger.

I tillegg må virksomheten løpende kontrollere at sikringstiltakene som er pålagt eller besluttet etablert faktisk er iverksatt og fungerer etter sin hensikt. Også når tiltak er implementert og har fått fungert en periode, er det viktig å kontrollere at tiltaket faktisk fungerer etter sin hensikt. Dette fungerer som den interne sikkerhetsrevisjonen og skal brukes som ett av grunnlagene i ledelsens årlige evaluering av sikkerhetstilstanden. Internrevisjon er for øvrig et krav etter ISO 27001.

Virksomhetens leder skal minst en gang i året evaluere sikkerhetstilstanden i virksomheten. Personopplysningsforskriften § 2-3 krever at bruk av informasjonssystemet skal jevnlig gjennomgås for å klarlegge om den er hensiktsmessig i forhold til virksomhetens behov, og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat.

En overordnet analyse av virksomheten bør gjennomføres med faste intervaller, f eks årlig, avhengig av virksomhetens objekter/informasjon og trusselbilde.

Avvikshåndtering er et element i revisjons- og kontrollarbeidet. Virksomheten skal sikre at prosedyrer for avviks- og endringshåndtering foreligger og følges. Prosedyrene for dette skal omfatte alle avvik som oppstår i driften av informasjonssystemene og skal ha som formål å gjenopprette normal tilstand i virksomheten. Avviksbehandlingen skal identifisere årsaken til avvik, hindre gjentakelser og sikre forsvarlig og formell behandling av avviket. Avvikene skal dokumenteres.

Virksomheten skal etablere en prosedyre for kontinuitet hvor roller, ansvarsoppgaver og risiko defineres. En kontinuitetsplan bør blant annet inneholde identifisering og vurdering av enkeltelementer som kan svikte og iverksette tiltak, klare kriterier for oppstart av reserveløsningen gjenopprettingsprosedyrer informasjon til ledelse, ansatte, eventuelt kunder og leverandører. Det skal gjennomføres opplæring, øvelse og testing av reserveløsningene i et omfang som gir trygghet for at reserveløsningene fungerer tilfredsstillende. Testene skal dokumenteres slik at gjennomføring og resultat kan vurderes i ettertid.

Det er viktig å sikre at avvik i informasjonssystemene i det enkelte foretak behandles hurtig og etter en fastlagt prosedyre slik at normalsituasjonen

gjenopprettes og at tiltak iverksettes for å unngå at samme type hendelse skjer på nytt.

Når tiltak er godkjent av ledelsen, kan de implementeres. Det er viktig at ansvar for implementering blir bestemt for alle tiltak. Ansvarer kan ligge hos en enkeltperson eller en enhet. Noen tiltak vil kreve eksterne ressurser som for eksempel konsulentbistand. Slike tiltak må uansett ha en ansvarlig internt.

Alle tiltak må ha en frist for gjennomføring. Det bør besluttes et system for tilbakemelding når et tiltak er implementert.

Når tiltaket er implementert, skal dette oppdateres i de aktuelle planer og instruksjer.

6 Metode og kilder

Offentlige virksomheter benytter ulike risikovurderingsmetoder, både kvantitative og kvalitative. Bruk av kvalitative metoder for å innplassere hendelser er sjelden presise. Erfaringen viser imidlertid at metoden er nyttig for å identifisere nødvendige innsatsområder. De kvantitative metodene har en svakhet i at alt en lar inngå skal kvantifiseres (i form av tallverdier) for å kunne gjennomføre de nødvendige vurderinger. Dette blir raskt et omfangsrikt og tidskrevende arbeid. I tillegg kan det være komplisert å tallfeste konsekvenser som er vanskelige å måle, som for eksempel negativ påvirkning av omdømme. En måte å håndtere dette, er å angi hvor mye virksomheten er villig til å betale for å unngå at en bestemt hendelse inntreffer.

Svenske og danske offentlig virksomheter er direkte pålagt å oppfylle krav i standarder for styring av informasjonssikkerhet. I Danmark er dette DS 484, som er utarbeidet på basis av internasjonale standarder og ”best practice” for styring av informasjonssikkerhet og tilpasset danske forhold. I Sverige skal SS-ISO/IEC 27001:2006 og SS-ISO/IEC 27002:2005 legges til grunn. I Norge har hovedtyngden av regelverket basis i samme ISO-standard. Om standarder se [Standard.no](#).

Det er skrevet mye om risikohåndtering, risikostyring og risikovurderinger. I denne veiledningen er derfor mye av innhold og ideer hentet fra det andre har skrevet. Veiledningen er forsøkt tilpasset offentlig sektors behov for risikovurderinger knyttet til autentisering og uavviselighetsproblematikken. Det legges opp til en kombinasjon av metoder, hvor risikobildet beskrives både tekstlig (kvalitativt) og med tall (kvantitativ), ved at sannsynlighet, konsekvens og risiko plasseres i et begrenset antall intervaller.

Spesielt mye er hentet fra Datatilsynets veiledning om risikovurdering av informasjonssystem og Nasjonal Sikkerhetsmyndighets (NSM) veiledning i risiko- og sårbarhetsanalyse. Metodisk er [Datatilsynets veiledning i risikovurderinger](#) spesielt velegnet. Begreper, oppsett og vurderinger er i dette dokumentet i stor grad sammenfallende med denne. Personopplysninger som vurderingstema er, i veiledningen her, utvidet til også å omfatte virksomhetens øvrige verdier hvor informasjonssikkerheten har betydning. Håndtering av de ulike typer konsekvenser (økonomisk skade, personvernskade, tap av tillit og omdømme, osv) gjøres relevante. Av samordningshensyn er også skala og begreper benyttet i Datatilsynets, allerede innarbeidede, veiledning for vurdering av sannsynlighet og konsekvens benyttet her.

Metodene det her legges opp til er ikke avhengig av virksomhetsstørrelse. Det vil være virksomhetens valg av ressurser, situasjoner og trusseltyper, samt de involvertes kompetanse, som avgjør kostnadene ved gjennomføring av vurderinger. Særskilte krav inntatt i særlovgivning kan innarbeides i denne systematikken.

Videre er det tatt utgangspunkt ISO (The International Organization for Standardization) 27001, 27005 og 31000. For ytterligere informasjon se www.standard.no.

Den danske IT- og Telestyrelsen har utarbeidet en hjemmeside hvor det presenterer flere redskaper som kan være til hjelp i arbeidet med å styre virksomhetens informasjonssikkerhet. Der er det også [enkelte sjekklister](#) som kan være egnet som et utgangspunkt i dette arbeidet⁵.

For øvrig er det hentet inspirasjon fra Asker kommune og Utlendingsdirektoratet (UDI) og Statens lånekasse for utdanning.

⁵ Se: <http://www.itst.dk/it-sikkerhed/ds-484>

Vedlegg 1 - Relevante lover og forskrifter

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) [§ 13](#), som stiller krav om utarbeidelse av sikkerhetsmål og sikkerhetsstrategi, er sentral rettslig sett. Sikkerhetsmål og strategi skal utarbeides i henhold til ”anerkjente prinsipper”, som grunnlag for forvaltningsorganenes beslutninger om innføring og bruk av sikkerhetstjenester og – produkter på en planlagt, helhetlig, systematisk og dokumentert måte. Dette kravet forutsetter at risikovurderinger inkluderes og gjennomføres, og at slike vurderinger gir grunnlag for forholdsmessige tiltak.

Krav om risikovurderinger gjelder virksomheten generelt, og som en del av denne helheten må risikovurderingene omfatte og inkludere autentisering og uavviselighet spesielt. Et forvaltningsorgan kan iht forskriften § 4, (2) og (3) be om opplysninger som bekrefter identiteten til en som henvender seg til forvaltningen elektronisk, eller stille krav om at det skjer på en bestemt måte, eller på et bestemt sikkerhetsnivå, hvis ”dette er av betydning for håndteringen av henvendelsen”. Forvaltningsorganet kan videre bestemme at ”nærmere angitte typer av henvendelser” generelt skal følge de angitte måtene og sikkerhetsnivåene, som organet har kommet frem til, men disse må være basert på organets risikovurderinger og sikkerhetsstrategi.

Videre pålegger [personopplysningsloven § 13](#) den behandlingsansvarlige å sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet. Det vil si etablering av sikkerhetstiltak i forhold til faktisk risiko. Risikovurderinger er sentrale i oppfyllelsen av kravene. Det følger av [personopplysningsforskriften § 2-4](#) at risikovurdering skal gjennomføres ” ... for å klarlegge sannsynlighet for og konsekvens av sikkerhetsbrudd ... ”. Det følger også at det er virksomheten selv som må fastlegge kriterier for hva den anser som akseptabel risiko forbundet med behandlingen av personopplysninger Dokumentasjon på at risikovurdering er gjennomført skal være tilgjengelig for tilsynsorganer.

Sikkerhetstiltakene skal stå i forhold til sannsynligheten og konsekvensen av sikkerhetsbrudd. Det finnes en rekke verktøy til hjelp ved vurdering av risiko. Mange er imidlertid svært omfattende, med fokus på detaljert og formell metodikk. Risikovurderingene skal ikke være mer omfattende eller formalisert enn nødvendig, se for eksempel Datatilsynets merknader (til § 2-4 i [Sikkerhetsbestemmelsene i personopplysningsforskriften](#)) og økonomiregelverkets krav om at interkontrollen skal være tilpasset vesentlighet og risiko ([Bestemmelser om økonomistyring i Staten](#), kap 2.2).

Arbeid med å håndtere risiko er som hovedregel pålagt i lov eller forskrift.

- For behandling av personopplysninger gjelder [§ 2-4](#) i forskrift til personopplysningsloven, om at en behandlingsansvarlig skal gjennomføre en risikovurdering. Datatilsynet er tilsynsmyndighet for denne forskriften, og har laget en veiledning til arbeidet med å foreta en risikovurdering. Begrepet risikovurdering er valgt i stedet for det mer formelle uttrykket risikoanalyse, for å markere at omfanget og formaliseringsgraden på vurderingen skal være tilpasset behovet.

-
- For virksomhet som er underlagt tilsyn av Kredittilsynet gjelder forskrift om bruk av informasjons- og kommunikasjonsteknologi av 21. mai 2003 nr 630. Hvem denne forskriften gjelder for er beskrevet i [forskriftens § 1](#). I denne [forskriftens § 3](#) beskrives krav til gjennomføring av risikoanalyse. Les mer om risiko- og sårbarhetsanalyser for finansforetak.

Også andre regelverk stiller tilsvarende krav på sine områder, se bl.a. [forskrift om sikkerhetsadministrasjon § 4-1](#).

Vedlegg 2 - Anbefalinger

Rammeverkets fire risikonivåer

Rammeverket definerer fire felles risiko- og sikkerhetsnivåer for autentisering og uavviselighet tilpasset offentlig sektor. Offentlige virksomheter skal, på bakgrunn av risikovurderinger, kunne plassere egne tjenester/samhandling i henhold til disse felles risikonivåene. Dette skal igjen danne grunnlag for valg av riktig sikkerhetsnivå, hvor det, basert på behov for sikkerhet og funksjonalitet, kan velges en egnet løsning for autentisering eller uavviselighet. Den valgte løsningen bør gjøre det så vanskelig å misbruke tjenesten at den resterende risikoen anses som forholdsmessig akseptabel. De fire definerte risikonivåene beskrives som produktet av identifisert konsekvens og sannsynligheten for at den inntreffer.

Formålet med de fire predefinerte risikonivåene er å legge til rette for felles løsninger, og gjenbruk av løsninger, for autentisering og uavviselighet. Risikonivåene i rammeverket beskrives i form av konsekvenser. Risikoen, som er produktet av sannsynlighet og konsekvens, blir dermed beskrevet som konsekvenser som er inkludert eller ekskludert avhengig av sannsynligheten.

Sikkerhetsnivåer for autentisering og uavviselighet

Sikkerhet i løsninger for autentisering og uavviselighet kan beskrives ved hjelp av forskjellige sikkerhetsparametere. En sikkerhetsparameter er en faktor som påvirker sikkerhetsnivået i løsningen hvis den endres. Et eksempel på slik faktor er ”utlevering til bruker”. For en passordløsning vil ”utlevering til bruker” beskrive hvordan passordet i praksis deles ut til brukeren. Er passordene delt ut til bruker på bakgrunn av fysisk legitimering, er det vanskelig å skaffe seg et passord i andres navn. Deles passordene ut over Internett på bakgrunn av påstått identitet er det lett å skaffe et passord i andres navn. Ulike krav til samme sikkerhetsparameter endrer på denne måten graden av hvor vanskelig det er å kompromittere løsningen.

Sikkerhetsnivåene i [rammeverket](#) er definert på bakgrunn av følgende sett av sikkerhetsparametere:

- **Krav til autentiseringsfaktor(er)**
Beskriver antall autentiseringsfaktorer og deres egenskaper. For eksempel om autentiseringsfaktoren er statisk eller dynamisk. Med statisk menes at dokumentasjonen som presenteres for andre som skal verifisere påstått identitet ikke endres fra gang til gang. Et eksempel på dette er fast passord eller biometriske data. Med dynamisk menes at dokumentasjonen som presenteres for andre som skal verifisere påstått identitet, endres fra gang til gang. Eksempler på slike løsninger er tidsbaserte passordkalkulatorer, som gir nytt passord avhengig av tid, og løsninger basert på PKI, hvor det ved hver autentisering genereres en ny, tilfeldig datastreng som signeres digitalt.

-
- Utlevering til bruker
Beskriver hvordan man sikrer knytningen mellom autentiseringsfaktorer og brukeridentiteter. For eksempel om brukeren har måttet møte opp fysisk og legitimere seg selv, eller om brukeren har fått noe tilsendt til folkeregistrert adresse.
 - Sikring av autentiseringsfaktorer ved lagring
Beskriver hvordan autentiseringsfaktoren er lagret lokalt, og hvordan den er fysisk og logisk sikret. Et eksempel er forhåndsdefinerte passordlister. Kommer disse på et åpent ark, er de kopierbare. Er passordene beskyttet som skrapelodd, er de ikke kopierbare uten at mottakeren vil oppdage dette.
 - Krav til uavviselighet
Beskriver i hvilken grad det i ettertid er mulig å dokumentere at en bruker står bak et informasjonselement eller har utført en handling.

Innebærer at det finnes en offentlig kravspesifikasjon (ev. en forvaltningsstandard) for den type løsninger, og at løsningen er deklarerert ved en offentlig ordning.

Settet med sikkerhetsparametrene som er benyttet i Rammeverket er vektet slik at en løsning som skal tilfredsstillere ett sikkerhetsnivå, oppfyller kravene som er satt for alle sikkerhetsparametrene på dette nivået. Sikkerhetsparametre som er benyttet for å skille mellom sikkerhetsnivå er teknologinøytrale, men ikke uttømmende. Det forekommer autentiserings- og uavviselighetsløsninger som har andre sikkerhetsparametre som kan ha forskjellig nivå, og som dermed kan oppfattes sikkerhetsmessig forskjellig.

Se eksempel Nettvett.no

Vedlegg 3 - Forslag til skjema og utfyllingsveiledning

Forhold og krav	Krav og forhold som er viktige for informasjonssikkerheten vurderes og føres inn først. Dette kan være lover, forskrifter, prosesser, rutiner/prosedyrer, system, arkiv, lokaler osv.
Trusselbeskrivelse	Kort beskrivelse av trusselbildet – hva kan skje? Uønskede mulige situasjoner, hendelser eller handlinger som kan oppstå og som kan representere en fare for informasjonssikkerheten. Mulige konsekvenser for brukere, økonomi, ansatte, omdømme osv beskrives kort. Kan uttrykkes i tekst eller kostnader.
Sannsynlighetsgradering (S)	Hvor stor sannsynlighet er det for at trusselen inntreffer (hvor ofte forventes den uønskede hendelsen å inntreffe -frekvens)? S=4: Svært sannsynlig (hendelsen inntreffer flere ganger hvert år) S=3: Meget sannsynlig (hendelsen inntreffer årlig eller sjeldnere) S=2: Sannsynlig (hendelsen inntreffer en gang pr 10 år eller sjeldnere) S=1: Lite sannsynlig (hendelsen inntreffer en gang per 50 år eller sjeldnere) Merk: Angivelsen av frekvens/antall må tilpasses virksomheten og tjenesten som vurderes. Bruken (volumet) av tjenesten som skal risikovurderes er sentralt.
Konsekvensgradering (K)	Hvor alvorlige vil konsekvensen/skaden kunne være? K=4; Katastrofalt K=3; Kritisk K=2; Farlig (kan være uheldig) K=1; Lite farlig (dette lever vi godt med) Et utgangspunkt for vurderingen kan være hva som skal til for å gjenopprette. Konsekvensgradering av at lover/forskrifter ikke blir oppfylt, settes alltid til høyt.
Tiltak	Risikoen er produktet av S og K. Akseptabelt risikonivå skal være nedfelt i virksomhetens sikkerhetspolicy. Dersom risikoen er større eller lik det akseptable nivå (for eksempel $K \times S \geq 8$) skal det iverksettes risikoreducerende tiltak (tiltak som reduserer sannsynligheten eller konsekvensene av uønsket hendelse). Gjennomføring av tiltak bør knyttes til en kost-nytte-vurdering. Når tiltaket skal være gjennomført og hvem som er ansvarlig, bør føres inn. Hvis tiltaket ikke er gjennomført innen fristen skal det registreres som avvik.
Forventet effekt av tiltak	Før inn forventet ny risiko etter at planlagt tiltak er gjennomført.
Opplevd effekt av tiltak	Før inn opplevd ny risiko etter at planlagt tiltak er gjennomført. Hvis tiltaket ikke har hatt den ønskede effekten, må nytt tiltak vurderes iverksatt.

