



Veilder risikovurdering

Dette dokumentet skal være en hjelp til gjennomføring av en risikovurdering. Veilederen benytter eksempler som best passer en virksomhet i helsesektoren. Det er viktig at resultatet av risikovurderingen blir dokumentert. Eksempel på slik risikorapport finnes på <http://www.nhn.no/informasjonssikkerhet> under risikovurdering.

Det vises også til Faktaark 5 - Fastsettelse av akseptkriterier for tilgjengelighet, konfidensialitet og integritet Versjon 2.0 og Faktaark 7 - Risikovurderinger som ligger på www.normen.no .

Innhold

1. System/tjenestebeskrivelse	3
2. Hvem utgjør truslene?	3
3. Hva frykter vi skal skje?	3
4. Hvordan kan hendelsen inntreffe	4
5. Hvilke sårbarheter gjør dette mulig?	4
6. Sannsynlighet, konsekvensvurdering og trusselhåndtering	4
7. Innplassering i tabell og matrise for risikovurdering (Risikomatrise)...	5
8. Vurdering av tiltak.....	5
9. Ordliste.....	6

Stegene i risikovurderingen

1. System/tjenestebeskrivelse

En overordnet beskrivelse av systemet/tjenesten som skal risikovurderes

Eksempel:

- i. Systemskisse/tjenestebeskrivelse*
- ii. Dataflyt*
- iii. Rollebeskrivelse*
 - 1. Systemeier*
 - 2. Databehandleransvarlig*
 - 3. Databehandler*
- iv. Hvilke data behandles?*
 - 1. Sensitiv*
 - 2. Åpen*

2. Hvem utgjør truslene?

Eksempel:

- i. Bruker*
 - 1. Med vilje*
 - 2. Utsiktet (hendig uhell)*
- ii. Hackere*
- iii. Driftspersonell*
 - 3. Med vilje*
 - 4. Utsiktet (hendig uhell)*
- iv. Systemet/tjenesten*
 - 5. Uønsket funksjonalitet*
 - 6. Misbruk av tjenesten*

3. Hva frykter vi skal skje?

Eksempel:

- i. Data på avveie* *Konfidensialitet*
 - 1. Data kommer i hendene på hacker*
 - 2. Bruker uten gyldig tilgang får se data*
- ii. Endring av data* *Integritet*

- 3. *Bevisst manipulasjon*
- 4. *Systemfeil*
- iii. *Manglende tilgang til data* *Tilgjengelighet*
- 5. *Manglende redundans*
- 6. *Rettighetsproblemer*

4. Hvordan kan hendelsen inntreffe

Eksempel:

- i. *Feilkonfigurering av systemet/tjenesten*
- ii. *Hacker benytter sårbarhet i systemet/tjenesten*
- iii. *Brukere har onde hensikter*

5. Hvilke sårbarheter gjør dette mulig?

Eksempel:

- i. *Manglende brannmur*
- ii. *Manglende oppdatering av Operativsystemet og Software*
- iii. *Manglende kunnskap om løsning/tjeneste hos bruker*
- iv. *Manglende testrutiner hos driftspersonell*
- v. *Uønsket funksjonalitet i løsningen/tjenesten*

6. Sannsynlighet, konsekvensvurdering og trusselhåndtering

Hvor sannsynlig er det at hendelsen inntreffer?

Eksempel:

- i. *Hvor ofte vil en hendelse kunne inntreffe*
- ii. *Hvilke tiltak er innført for å hindre en hendelse*
 - 1. *Brannmur installert mellom sonene*
 - 2. *Tilgangskontroll*
 - 3. *Uønsket funksjonalitet slått av*
 - 4. *Opplæring av brukere*
 - 5. *Avtalemessige avgrensninger*

Hvilken konsekvens har hendelsen hvis den inntreffer?

Eksempel:

- i. Er det fare for liv og helse?*
- ii. Har det økonomiske konsekvenser?*
- iii. Skader det organisasjonen sitt omdømme?*

7. Innplassering i tabell og matrise for risikovurdering (Risikomatrise)

Se mal for risikovurdering. Her skal resultatet innplasseres i tabeller og en risikomatrise lages ut i fra dette.

8. Vurdering av tiltak

Hvilke tiltak kan settes inn for å dekke risikoen som ikke er innenfor akseptanse-kriteriene

9. Ordliste

Med "**systemskisse**" menes en tegning som viser hvordan systemet er satt sammen. Hvilke deler systemet består av, og hvordan disse henger sammen.

Med "**dataflyt**" menes en beskrivelse av hvordan datatrafikken "flyter" i systemet/tjenesten. Her skal man f eks vise hvor data initieres fra og hvor den termineres.

Med "**systemeier**" menes den instansen som er juridisk eier systemet/tjenesten

Med "**databehandler**" menes den som *behandler helse- og personopplysninger* på vegne av den *databehandlingsansvarlige*, jf. [helseregisterloven § 2 nr. 9](#) og [personopplysningsloven § 2 nr. 5](#)). Det presiseres at en *databehandler* er en ekstern person eller virksomhet utenfor den *databehandlingsansvarliges* virksomhet. Det vil si at den *databehandlingsansvarliges* egne medarbeidere ikke er dennes *databehandlere*.

Med "**databehandlingsansvarlig**" menes den som bestemmer formålet med *behandlingen* og hvilke hjelpemidler som skal brukes, hvis ikke *databehandlingsansvaret* er særskilt angitt i loven eller i forskrift i medhold av loven, jf. [helseregisterloven § 2 nr. 8](#) og [personopplysningsloven § 2 nr. 4 \(her benyttes begrepet "behandlingsansvarlig"\)](#). Det presiseres at det er virksomheten som er *databehandlingsansvarlig* for *behandling av helse- og personopplysninger*. Ansvaret skal ivaretas av den daglige ledelsen av virksomheten, og virksomheten er pliktsubjekt.

Med "**hackere**" menes personer som med onde hensikter forsøker å utnytte svakheter i en løsning/tjeneste

Med "**integritet**" menes at *helse- og personopplysninger* må være sikret mot utilsiktet eller *uautorisert* endring eller sletting.

Med "**konfidensialitet**" menes at *helse- og personopplysninger* må være sikret mot at uvedkommende får kjennskap til opplysningene.

Med "**tilgjengelighet**" at *helse- og personopplysninger* som skal *behandles*, er tilgjengelig til den tid og på det sted det er behov for opplysningene.