

Risikoanalyse

Metodegrunnlag og
bakgrunnsinformasjon

Versjon 1.0
8. september 2000

KITH Rapport 13/2000
ISBN 82-7846-091-4

KITH-rapport

Tittel

Risikoanalyse

Metodegrunnlag og bakgrunnsinformasjon

KITH**Kompetansesenter for
IT i helsevesenet AS**

Postadresse

**Sukkerhuset
7489 Trondheim**

Besøksadresse

Sverresgt 15, inng G

Telefon

73 59 86 00

Telefaks

73 59 86 11

e-post

firmapost@kith.no

Foretaksnummer

959 925 496

Forfatter(e)

Bjarte Aksnes, Arnstein Vestad, Tor Olav Grøtan

Oppdragsgiver(e)

Sosial- og helsedepartementet

Rapportnummer

R 13/2000

URL

<http://www.kith.no/rapportarkiv/rosmet.pdf>

Prosjektkode

S-SV-ROS

ISBN

82-7846-091-4

Dato

8. sept 2000

Antall sider

21.

Kvalitetssikret av

Harald Norvik

Gradering

Åpen

Godkjent av

Jacob Hygen
Adm. direktør

Sammendrag

Risikoanalyse er et verktøy for å skape oversikt over verdier og trusler mot disse i en organisasjon eller informasjonssystem. Denne rapporten gir råd om hvordan arbeidet med risikoanalyser kan organiseres. Videre diskuteres hvordan akseptkriterier benyttes for å avgjøre hvilken risiko organisasjonen er villig til å utsette seg for, hvordan trusler mot systemene og organisasjonen identifiseres og vurderes mht. sannsynlighet og konsekvens.

Rapporten ser også risikoanalyser i sammenheng med BS 7799 – en britisk standard for informasjonssikkerhet, og gir skjema som hjelpemiddel for å beskrive trusler og vurdere risiko.

Innhold

INNLEDNING	2
HVORFOR GJENNOMFØRE EN RISIKOANALYSE?	2
Organisering av arbeidet	2
Akseptkriterium	3
Om metoden	3
IDENTIFISERING AV TRUSLER	4
SANNSYNLIGHETS-, KONSEKVENNS- OG RISIKOVURDERINGER.....	7
Konsekvenser	7
Eksempel	7
Sannsynlighetsvurdering	8
Risikovurdering	9
TILTAK OG OPPFØLGING	11
Ledelsens vurdering av tiltak, prioritering og handlingsplan	15
Revisjon og oppfølging	15
BS 7799 OG RISIKOANALYSE.....	17
Krav til risikoanalyse i BS7799	18
KRITISK VURDERING – HYPOTESER OG USIKKERHET	19
Referanser	21
RISIKOSKJEMA	22

Innledning

Det å gjennomføre en risikoanalyse er et verktøy for å bedre informasjonssikkerheten. Utgangspunktet for en satsing på informasjonssikkerhet er ofte lovpålagte krav, f.eks. Datatilsynets regelverk, men det kan også være et eget ønske om å bedre kvaliteten og sikkerheten for virksomhetens kjernevirksomhet. Det kan ofte være vanskelig å synliggjøre den virkelige verdien av dette arbeidet, og vi vil derfor peke på noen gode grunner for å gjennomføre en risikoanalyse:

En risikoanalyse vil peke på hvilken risiko man løper dersom nødvendige sikringstiltak ikke gjennomføres, og den kan gi forslag til hvilke tiltak som bør prioriteres, slik at ledelsen får et bedre beslutningsunderlag for det videre arbeidet. Risikoanalysen gir også verdifulle innspill til budsjettarbeid og planlegging, spesielt for IT-avdeling eller tilsvarende. En annen gevinst ved å gjennomføre en risikoanalyse kan være at bevisstheten og kunnskapen om informasjonssikkerhet høynes blant de ansatte, noe som i neste omgang kan gi en bedre informasjonssikkerhet.

Organisering av arbeidet

Arbeidet bør starte med å beskrive bakgrunn og mål for en risikoanalyse av informasjonssystemet. Virksomhetens ledelse bør delta aktivt i utformingen av denne beskrivelsen. Overordnet målsetning vil som regel være å få risikoen innenfor et akseptabelt nivå, og dette innebærer at ledelsen må være villig til å iverksette nødvendige tiltak dersom risikoanalysen avdekker at risikoen er for høy. En første gangs gjennomføring av en risikoanalysen vil normalt beskrive risikoen ved dagens organisasjon og systemer. Senere kan ny risikoanalyse gjennomføres i forbindelse med planlegging eller etter gjennomføring av vesentlige endringer i informasjonssystemet.

Risikoanalysen bør utføres av en arbeidsgruppe, som er sammensatt av personer som kjenner informasjonssystemet og virksomheten/enheten som systemet er en del av, samt personer med kunnskap om gjennomføring av risiko- og sårbarhetsanalyser (f.eks. eksterne konsulenter). Dersom det leies inn eksterne konsulenter for å hjelpe til med å gjennomføre risikoanalysen, bør det legges vekt på kompetanseoverføring til interne personer, slik at disse selv kan gjennomføre analyser siden. En del virksomheter har gjennomført risiko eller sårbarhetsanaly-

ser i forbindelse med år 2000-arbeidet, og det bør derfor finnes en del kompetanse blant de som har deltatt i dette arbeidet.

Arbeidet med risikoanalysen bør organiseres som et prosjekt med en prosjektleder som rapporterer til ledelsen eller en styringsgruppe (med representanter fra ledelsen). Arbeidsgruppen bør få et klart mandat for arbeidet. En risikoanalyse bør taushetsbelegges, fordi den normalt vil avdekke svakheter og sikkerhetskritiske forhold for analyseobjektet. Deltagerne i gjennomføringen bør av samme grunn avlegge taushetserklæring. Selv om den enkelte risikoanalysen er taushetsbelagt, bør det legges vekt på å dele informasjon om årsaks- og risikoforhold med lignende virksomheter, f.eks andre sykehus.

Akseptkriterium

Dersom det finnes tilstrekkelig grunnlag for det bør det settes opp akseptkriterier før analysen gjennomføres. Alternativt kan akseptkriteriene settes opp etter første gjennomgang av en risikoanalyse. Et akseptkriterium angir at man aksepterer risikoen knyttet til en hendelse, dersom:

- Sannsynligheten for at hendelsen inntreffer er tilstrekkelig lav og/eller
- Konsekvensene av hendelsene er tilstrekkelige ufarlige (evt kan kontrolleres)

Resultatet av en risikoanalyse må vurderes opp mot de akseptkriterier virksomheten har satt seg. Akseptkriteriene uttrykker grensen mellom hva som er akseptabel risiko og hva som er uakseptabelt, og må fastsettes av virksomhetens ledelse på bakgrunn av bla. de krav og rammebetingelser som virksomheten er underlagt gjennom lovverk, forskrifter osv. På de områder hvor den risikoen som er avdekket ligger utenfor akseptkriteriene vil det være nødvendig å sette inn tiltak. Akseptkriterier vil som regel være individuelle for hver enkelt virksomhet, men det kan være nyttig å ta utgangspunkt i etablert praksis i lignende virksomheter.

Om metoden

I resten av rapporten vil vi beskrive en metode og et rammeverk som kan benyttes for å gjøre risikoanalyser. Den beskrevne metodikken kan benyttes både for tilfeldige hendelser (safety) og hendelser som er resultat av viljestyrte handlinger utført av mennesker (security), men hovedfokuset vil ligge på security-området. Vi tar også utgangspunkt i kvalitativ tilnærming, fordi det er svært vanskelig å basere seg på utelukkende kvantitative tilnærminger for hendelser der mennesker er involvert. Dersom man utelukkende ønsker å studere tilfeldige hendelser finnes det metodikk og verktøy som trolig er bedre egnet enn det som er beskrevet i denne rapporten.

Identifisering av trusler

Risikoanalysen bør starte med en enkel beskrivelse av analyseobjektet og hvilke avgrensninger som er foretatt. Spesielle forutsetninger og rammebetingelser må også beskrives. Ved en risikoanalyse av en organisasjons informasjonssikkerhet vil vi i hovedsak rette søkelyset mot uønskede hendelser / trusler rettet mot kravene til konfidensialitet, integritet, tilgjengelighet og sporbarhet. Man bør her være forsiktig med å blande årsakssammenheng med beskrivelse av truslene. En trussel kan ha flere ulike årsaker, en årsaksanalyse vil søke å finne så mange mulige årsaker som mulig som bakgrunn for å estimere sannsynligheten for at trusselen utløses.

Ulike ressurser kan benyttes som underlagsmateriale for denne prosessen:

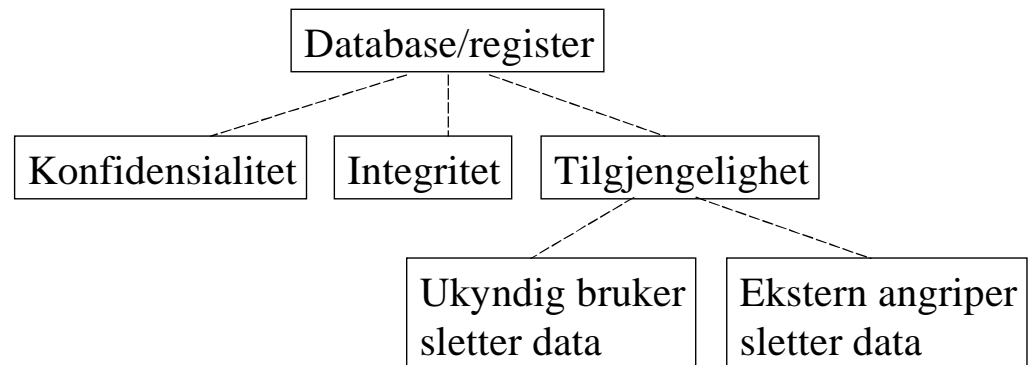
- Tidligere utførte Risiko eller sårbarhetsanalyser (f.eks. år 2000 arbeid)
- Beredskapsplaner/kriseplaner
- Strategier (IT-strategi etc)
- Systembeskrivelser/arkitektur og konfigurasjonskart
- Kommunikasjon med tilsynsmyndigheter (f.eks. Datatilsynet)
- Stillingsbeskrivelser/ organisasjonskart
- Opplæringsprogram/dokumentasjon
- Organisasjonens system for avvikshåndtering
- Lovpålagte krav
- Intervjuer med sentrale medarbeidere (IT-ansvarlig, Sikkerhetsansvarlig, IT-drift, ordinære brukere m.fl.)

I denne fasen av risikoanalysen er det særlig viktig at deltagere med god kjennskap til analyseobjektet deltar og gir innspill. For å komme frem til de viktigste truslene kan man kombinere flere ulike metoder og kilder, og det kan være naturlig å starte med en brainstorming eller idemyldring. I dette ligger det at deltakerne legger fram alle forslag de kan komme på,

uavhengig av om de vurderes som gode eller dårlige. Håpet i en slik prosess er at gruppen, ved å kombinere de ulike bakgrunner og ståsteder til medlemmene, kan komme fram til resultater som enkeltpersonene ikke ville komme fram til. Ved å oppfordre medlemmene til mest mulig ”hemningsløst” å komme med forslag øker man også at sannsynligheten for at gode forslag trer fram.

Selv om idemyldringen skal være mest mulig fristilt, er det likevel nyttig å gi gruppen et visst fokus for arbeidet. Noen stikkord kan være:

- List opp kritiske ressurser/verdier (inkludert ressurspersoner), og
- Knytt hendelsene til sted/system
- Vektlegg informasjonsressurser med sensitive personopplysninger eller virksomhetskritisk informasjon
- Se på hendelser med eksternt/internt opphav (innbruddstyv/medarbeider)
- Fokuser på konfidensialitet, integritet og tilgjengelighet til sentrale informasjonsressurser
- Ta utgangspunkt i den daglige arbeidssituasjonen



Figur 1 Hierarkisk nedbryting av trusler mot en informasjonsressurs

Ulike mer strukturerte metoder kan også tenkes brukt for å ”generere” mulige hendelser og trusler. Et eksempel er å utføre en hierarkisk nedbryting av de ulike truslene, sett med hensyn på de enkelte informasjonsressursene (se Figur 1). En slik nedbryting kunne for hvert informasjonsressurs se på hvilke trusler som er relevant for denne. Et eksempel kan ses i figuren over, hvor vi ser trusler mot tilgjengelighet brytes ned i to ulike hendelser, som man igjen kan studere konsekvens og årsak til. Tilsvarende framgangsmåte benyttes for de andre aspektene. En slik framgangsmåte kan klargjøre arbeidet med å komme fram til trusler, og bidra til at man ikke overser en del grunnleggende trusler. På den andre side kan selvsagt en slik strukturering virke hemmende på den frie

idéproduksjonen i en idémyldring. Det er derfor viktig å ikke la metoden være noen tvangstrøye, men heller en inspirasjonskilde.

Etter en idémyldring vil det forhåpentligvis foreligge en rekke mulige trusler/risikoelementer, hvor noen vil være mer relevant og aktuelle enn andre. Det er derfor naturlig å drøfte igjennom de ulike forslagene for å avgjøre hvilke som skal tas med videre i prosessen. Forslagene som ikke tas med bør begrunnes og dokumenteres, så man ikke bruker så mye tid på å vurdere de samme truslene ved en senere risikoanalyse.

Truslene kan som regel deles inn i fire hovedkategorier:

Overlagte – bevisste (ondsinnede eller vennligsinnede¹) handlinger utført av mennesker, herunder endring, utlevering eller sletting av informasjon samt tyveri/ødeleggelse av utstyr.

Utsiktede – en handling utført av et menneske som forårsaker en utilsiktet skade, dette kan f.eks. skyldes lite brukervennlige program, dårlige rutiner, komplekse driftsløsninger, manglende kompetanse, programmeringsfeil, manglende aktsomhet eller uhell.

Systemfeil – trussel som ikke **direkte** har sin årsak i en menneskelig handling eller naturkatastrofe, f.eks. diskkrasj, prosessorsammenbrudd, strømbrudd, lekkasje, eksplosjon/brann i virksomheten

Omgivelsesstyrte – trusler som har sin årsak i forhold i omgivelsene som vi i liten grad kan kontrollere som naturkatastrofer (oversvømmelse, ras, jordskjelv, orkan, høye/lave temperaturer), katastrofer og ulykker (krig, brann/eksplosjon i nærmiljøet med mer).

I tillegg kan trusler som er forårsaket av mennesker (enten det er overlagt eller utilsiktet) grupperes etter om de er forårsaket av interne eller eksterne personer. Det kan være nyttig å gå gjennom disse kategoriene for å se om man har tenkt på trusler fra alle disse fire hovedområdene.

¹ Vi tar også med vennligsinnede handlinger her, og vi sikter da til en handling som er i strid med gjeldende regelverk men som ikke har til hensikt å gjøre noen skade på verken virksomheten eller enkeltindivider, tvert imot.

Sannsynlighets-, konsekvens- og risikovurderinger

Kapittel

3

Vi bruker et skjema/mal (se vedlegg) for hver identifisert uønsket hendelse der vi ved hjelp av konsekvens- og sannsynlighetsvurderinger kommer frem til risikoen for hver enkelt hendelse. Skjemaet gir dessuten et godt grunnlag for å vurdere risikoreduserende tiltak.

Konsekvenser

For hver identifisert hendelse beskrives mulige konsekvenser og mulig hendelsesforløp. Det bør fokuseres på mulige skader på mennesker, informasjon og systemer. Husk på at en mulig konsekvens kan være kompromittering av informasjon om enkeltindivider (trussel mot personvernet). Det må også vurderes mulige konsekvenskjeder av en hendelse, f.eks. at en tilsynelatende ufarlig hendelse utvikler seg til en kritisk hendelse. For å vurdere dette må man ta hensyn til eksisterende skadebegrensende tiltak – disse må derfor beskrives. Til slutt angis alvorlighetsgraden for hendelsen (fra ufarlig til katastrofal).

Eksempel

Katastrofal – alvorlig og/eller akutt fare for større tap av kritisk informasjons integritet, tilgjengelighet eller konfidensialitet (som kan medføre fare for tap av liv eller helse)

Kritisk - alvorlig fare for tap av vesentlig informasjons integritet, tilgjengelighet eller konfidensialitet

Noen fare – hendelse som under gitte omstendigheter kan føre til noen skader

Ufarlig – ureglementert hendelse uten betydelige sikkerhetsmessige konsekvenser

Det kan være aktuelt å operere med flere konsekvensklasser, kategorisert etter hvilke område den uønskede hendelsen kan true. Konsekvensklasser kan f.eks være tap av henholdsvis konfidensialitet, integritet eller tilgjengelighet. I dette tilfelle må alvorlighetsgraden for hver konsekvensklasse angis, og det må etableres ulike kriterier for hver av klassene.

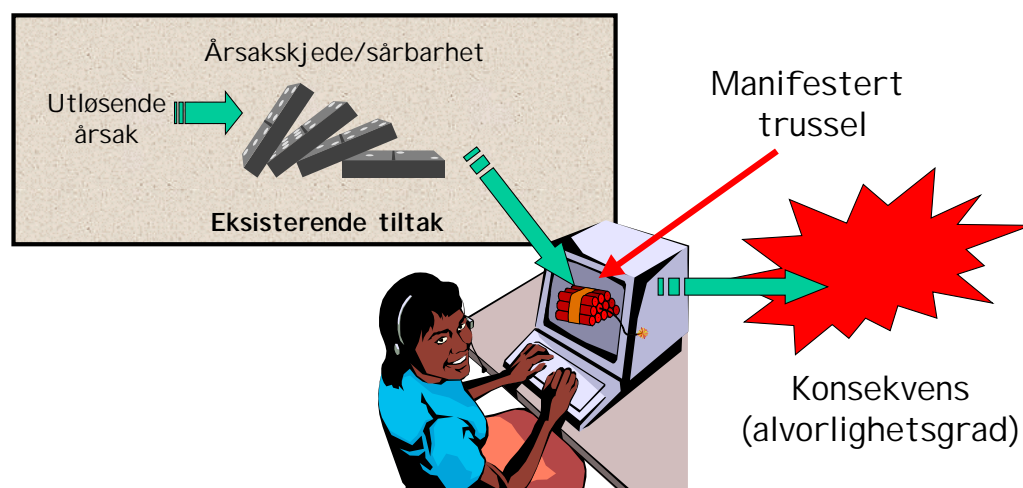
Sannsynlighetsvurdering

For hver uønsket hendelse må vi beskrive (mulige) årsaker til hendelsen og vurdere sannsynligheten for at disse vil inntreffe. For hendelser som er forårsaket av mennesker bør vi også beskrive hvem som kan være potensielle utførende aktører og hvilke motiver og muligheter (f.eks. kompetanse, utstyr, tid, økonomi) til å utløse hendelsen disse kan tenkes å ha.

Vi bør dessuten forsøke å identifisere mulige årsakskjeder, sekvenser eller kombinasjoner av hendelser som kan føre til en uønsket hendelse. Kjennskap til slike sammenhenger kan det lettere å finne forebyggende tiltak for å hindre at hendelsen oppstår, og det bidra til å fastsette sannsynligheten for hendelsen.

For å beskrive sannsynligheten må vi dessuten ha en oversikt over allerede iverksatte tiltak for å redusere sannsynligheten for hendelsen. Forebyggende tiltak må derfor beskrives, dersom slike finnes.

Når vi har en oversikt over årsaker og iverksatte forebyggende tiltak, kan vi anslå sannsynligheten for at hendelsen vil oppstå. For å vurdere sannsynligheten kan vi benytte erfaring fra egen eller lignende virksomheter og angi hvor ofte vi tror at hendelsen vil skje i løpet av en viss tidsperiode (f.eks. 10 ganger per år). Dersom publiserte frekvenstill fra undersøkelser, forsikringsselskaper el. er tilgjengelig kan man ta utgangspunkt i disse. En alternativ fremgangsmåte er å angi hvor lett en uønsket hendelse kan inntreffe, f.eks. hvor store ressurser som trengs for å komme forbi en sikkerhetsbarriere eller hvor robust et system er mot feilbetjening.



$$\text{Sannsynlighet}_{(\text{trussel})} \times \text{Konsekvens} = \text{RISIKO}$$

Sannsynligheten rangeres fra lite sannsynlig til meget sannsynlig, men hva man legger i de ulike begrepene må tilpasses lokale forhold (f.eks. som under).

Tabell 1 Sannsynlighet/frekvens

Begrep	Frekvens/sannsynlighet
Meget sannsynlig	Flere ganger pr. år
Sannsynlig	Ca 1 gang pr. år
Mindre sannsynlig	Ca 1 gang pr 3 år
Lite sannsynlig	Mindre enn 1 gang pr 3 år

Risikovurdering

Risiko vil vi definere som produktet av sannsynligheten for og konsekvensen av en uønsket hendelse. Vi kan plote hver hendelse inn i et risikodiagram som angir sannsynlighet på y-aksen og konsekvens på x-aksen.

Tabell 2 Risikodiagram m/akseptkriterier

Sannsynlighet	Konsekvens			
	Ufarlig	Noe farlig	Kritisk	Katastrofal
Meget sannsynlig				
Sannsynlig				
Mindre sannsynlig				
Lite sannsynlig				

I risikodiagrammet kan vi også angi akseptkriteriene:

Lav risiko	Middels risiko	Høy risiko
------------	----------------	------------

Lav risiko – Aksepteres uten videre, men åpenbare risikoreduserende tiltak kan vurderes.

Middels risiko – Risikoreduserende tiltak *bør* vurderes, eventuelt må ytterlige analyse foretas. Tiltak må vurderes utifra kost-nytte vurderinger.

Høy risiko – Ikke akseptabel risiko. Risikoreduserende tiltak **må** vurderes og iverksettes.

Når vi har kommet frem til risikonivået for hver enkelt hendelse kan vi vurdere om risikoen er innenfor akseptkriteriene, men vi kan ikke alltid se hver enkelt hendelse isolert fra de andre. Det vil ofte være sammenhenger mellom ulike hendelser, og det kan i *enkelte tilfeller* være nødvendig å akseptere en høyere risiko for en type hendelse for å få

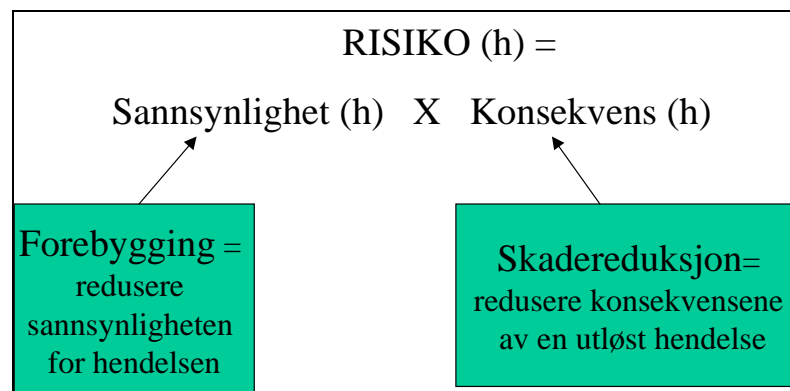
risikoen for en annen type hendelse ned på et akseptabelt nivå. I slike tilfeller må disse avveiningene dokumenteres og begrunnes.

Dersom vi benytter flere konsekvensklasser (f.eks konfidensialitet, integritet og tilgjengelighet), kan vi sette opp en risikomatrix for hver av konsekvensklassene. Det vil da være lettere å se hvilke hendelser som truer hver konsekvensklasse mest. Det bør også presenteres en samlet risikomatrix som viser den alvorligste konsekvensklassen for hver uønsket hendelse.

Tiltak og oppfølging

Risikoreduserende tiltak er tiltak for å redusere risikoen til et akseptabelt nivå. Dersom vi gjennom risikoanalysen avdekker at risikoen for en hendelse er på et uakseptabelt nivå, må virksomheten iverksette risikoreduserende tiltak. Det er to hovedtyper av risikoreduserende tiltak:

- Forebyggende – som har til hensikt å redusere sannsynligheten for hendelsen
- Skadebegrensende – som har til hensikt å minske skadevirkningene (konsekvensene) ved en uønsket hendelse og raskest mulig komme tilbake til normalsituasjonen



Figur 2 Risiko og risikoreduserende tiltak

Tiltakene kan f.eks. være innføringen av nye tekniske systemer, opplæringsaktiviteter, beredskapsøvelser, organisasjonsendringer, innføring av rutiner eller prosedyre. I alle fall må de iverksatte tiltakene ha som hovedmålsetning å få risikoen ned på et akseptabelt nivå (innenfor akseptkriteriene).

Forebyggende tiltak går ut på å redusere sannsynligheten for en uønsket hendelse ved å redusere/eliminere selve trusselen eller ved å redusere/eliminere svakheter som kan utløse hendelsen. Man kan f.eks. fjerne svakheter som kan utløse en uønsket hendelse ved å installere sikkerhetsoppdateringer av programvare eller operativsystem.

Som regel bør forebyggende tiltak vurderes før skadebegrensende tiltak, men dette må vurderes opp mot kost/nytte av de ulike tiltakene. Ofte kan det være aktuelt å iverksette begge typer tiltak rettet mot en og samme hendelse. Vi vil sjelden klare å eliminere sannsynligheten for en hendelse helt, og det kan kreve uforholdsmessig mye ressurser å f.eks. redusere sannsynligheten fra mindre sannsynlig til lite sannsynlig, det kan derfor ofte være mer fornuftig å bruke de siste kronene på skadebegrensende tiltak.

Eksempler på forebyggende tiltak:

- Innføring av sikkerhetsbarrierer (brannmurer)
- Bruk av virusprogramvare
- Konfigurasjonskontroll
- Systemer for logging og overvåkning (preventiv effekt)
- (Trussel om) bruk av sanksjoner ved overlagte sikkerhetsbrudd
- Opplæring av brukere og driftspersonale

Skadebegrensende tiltak går ut på å redusere skadevirkningene av en realisert trussel, men kan også omfatte tiltak for å komme raskest mulig i en normalsituasjon etter en uønsket hendelse, slik at konsekvensene ved å ikke ha informasjonssystemene tilgjengelig begrenses

Et viktig skadebegrensende tiltak kan være å redusere verdien til de ressursene som er utsatt for risiko, f.eks. ved å anonymisere eller kryptere informasjon. For hendelser med katastrofal eller kritisk konsekvens kan det være aktuelt å utarbeide katastrofeplan (kriseplan), eventuelt å oppdatere eksisterende katastrofeplan til å ta hensyn til hendelser i informasjonssystemet.

Eksempler på skadebegrensende tiltak:

- Kryptering av sensitiv informasjon
- Gode rutiner for reservekopiering
- Dublering av utstyr, linjer
- Service- og supportavtaler med leverandører
- Kritiske reservedeler lett tilgjengelig
- Rask varsling ved kritiske hendelser (indikatorer)

Merk! Det kan også være tilfeller der en ikke klarer å redusere risikoen (betydelig) for en hendelse med i utgangspunktet høy risiko, der man likevel velger å ta en "kalkulert risiko" fordi hendelsen ikke lar seg

eliminere uten at dette legger alvorlige hinder for virksomhetens kjernevirksomhet.

Risikoanalysen bør munne ut i en prioritert handlingsplan for ulike risikoreducerende tiltak, men det må være opp til ledelsen å ta den endelige beslutningen om hvilke tiltak som skal iverksettes.

Strakstiltak - En del tiltak kan og bør iverksettes umiddelbart fordi disse krever små endringer og lite ressurser. Spesielt bør strakstiltak som kan redusere risikoen betydelig iverksettes så raskt som mulig.

Langsiktige tiltak – Andre tiltak krever større endringer i systemer, infrastruktur eller organisasjon. Det kan også være nødvendig med til dels store investeringer i teknisk utstyr eller behov for tilførsel av kompetanse i form av nyansettelser, opplæring eller innleie av arbeidskraft. Disse tiltakene vil naturlig nok ha mer langsiktig karakter, og må også underlegges en grundigere kost-nytte vurdering.

Det kan dessuten ofte være aktuelt å iverksette strakstiltak for å redusere risikoen noe i en periode inntil langsiktige tiltak som kan redusere risikoen permanent er gjennomført.

Ulike tiltak kan dessuten deles inn i tre hovedkategorier:

- *Logiske (systemtekniske) tiltak* – f.eks. tilgangskontroll, sikkerhetsbarrierer, logging og overvåkning (IDS), redundans av ressurser
- *Fysiske tiltak* – f.eks. områdesikring, låser, alarmer, videoovervåking, merking av utstyr
- *Administrative tiltak* – f.eks. regler, prosedyrer, rutiner, opplæring, øvelser, testing

For hver av hovedkategoriene av tiltak bør vi identifisere hvilke tiltak som allerede er iverksatt, og for hvert av sikkerhetstiltakene vurdere om det har sitt motstykke i en trussel. På denne måten kan vi også avdekke sikkerhetstiltak som har utspilt sin rolle.

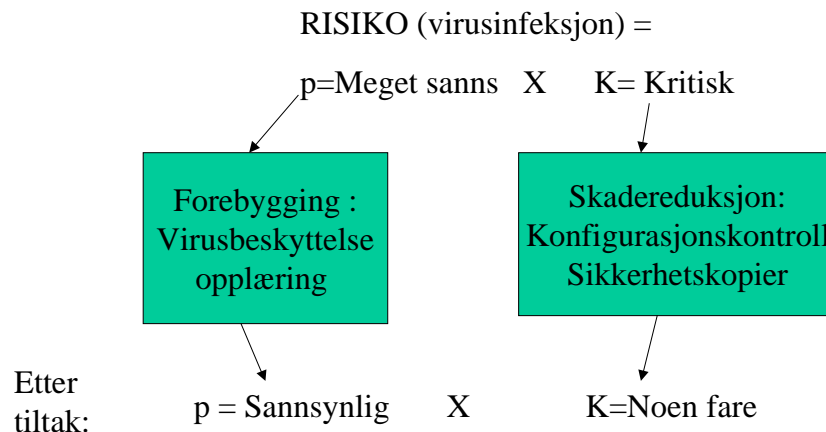
Det er i hovedsak tre strategier for risikoreduksjon: Risikounngåelse, risikooverføring og risikokontroll. Risikounngåelse dreier seg om å ta utgangspunkt i de reelle brukerbehovene, og velge de løsningene som gir lavest risiko. For eksempel kan dette være å velge løsninger med lav risiko, hvis disse fyller de behov man har, selv om det eksisterer løsninger som gir kan gi bedre ytelse, funksjonalitet osv., men som det er knyttet større risiko til.

Risikooverføring vil si å overføre kilder til risiko fra en del av et prosjekt / system til en annen del. Dette kan f.eks. være å la et system for adgangskontroll utføres av mennesker i stedet for av maskiner, slik at sannsynligheten for at feil person slippes inn reduseres.

Det tredje alternativet for risikoreduksjon er risikokontroll, dvs. å akseptere at risikoen eksisterer, etablere planer for å håndtere den og legge alternative planer hvis risikoen ikke lar seg avverge.

Eksempel:

Vi skal med et eksempel illustrere hvordan risikoreducerende tiltak kan benyttes for å redusere risikoen for en hendelse til å ligge innenfor akseptkriteriene. Et sykehus har anslått at de vil rammes av datavirus flere ganger per år, dette betyr at denne hendelsen er meget sannsynlig. Konsekvensene ved at sykehuset rammes av datavirus kan være kritiske dersom ingen tiltak er iverksatt, da dette kan ramme både integritet, tilgjengelighet og konfidensialitet til sykehuset informasjon. I tillegg kan det ramme sykehusets tillit og troverdighet hos pasienter og samfunnet generelt dersom det gjøres kjent at sykehuset ikke tar sikkerheten på alvor.



Figur 3 Virusinfeksjon: Forebyggende og skadereduserende tiltak

Plotter vi denne hendelsen inn i risikodiagrammet, ser vi at hendelsen faller innenfor *Høy risiko* området – noe som betyr at dette er en ikke-akseptabel risiko. Sykehuset iverksetter derfor forebyggende tiltak som innføring av programvare for virusbeskyttelse, samt opplæring av brukerne om hvordan unngå å bli smittet og spre virus. I tillegg iverksettes skadereduserende tiltak som konfigurasjonskontroll for lettere å kontrollere endringer i oppsett og programvare, samt sikkerhetskopiering av kritiske data, slik at disse kan gjenopprettes etter en eventuell infeksjon. Dette vil kunne redusere risikoen til *Middels risiko*, noe som sykehuset vurderer som akseptabelt i denne sammenheng.

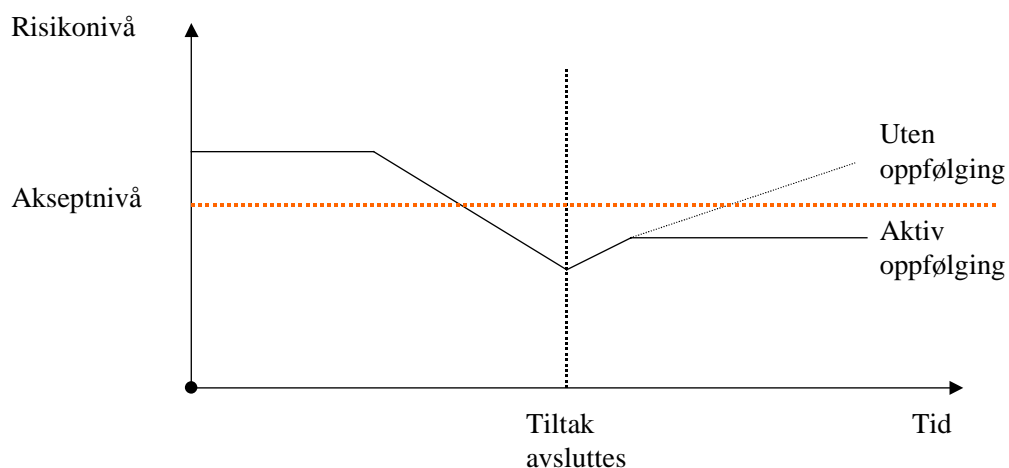
Tabell 3 Risikodiagram - risiko før og etter risikoreduserende tiltak

Sannsynlighet	Konsekvens			
	Ufarlig	Noe farlig	Kritisk	Katastrofal
Meget sannsynlig			X (før)	
Sannsynlig		X (etter)		
Mindre sannsynlig				
Lite sannsynlig				

Ledelsens vurdering av tiltak, prioritering og handlingsplan

Etter at risikoanalysen med forslag til risikoreduserende tiltak er gjennomført, må resultatene framlegges for ledelsen. Ledelsen må ta stilling til om dagens risikobilde er akseptabel, og eventuelt hvilke tiltak som skal iverksettes. Det vil ofte være nødvendig å gjøre nye analyser og vurderinger av kost/nytte før en endelig prioritering og handlingsplan kan settes opp.

Revisjon og oppfølging



Etter gjennomføringen av en risikoanalyse og eventuelle strakstiltak for å få risikoen på et akseptabelt nivå, vil risikoen være på et akseptabelt nivå og bevisstheten om viktigheten av sikkerhet vil være høy. Men dersom analysen bare settes i hylla og analysen ikke følges opp med varige tiltak vil sikkerhetsbevisstheten avta med tiden, noe som kan gi en høyere risiko etter hvert. Det er derfor viktig at analysen revideres med jevne mellomrom (f.eks årlig), og spesielt ved større endringer i informasjons-

systemer eller sikkerhetsorganisasjonen, for å sjekke om de er endringer i forutsetningene som ligger til grunn for vurderingene som ble foretatt. Ny kunnskap og resultater fra avvikshåndtering el. kan også gi verdifull input tilbake, og kan gjøre det nødvendig å foreta nye vurderinger. En revisjon trenger ikke å bety at hele analysen gjennomgås på ny, men de deler som er relevante for endringene bør revurderes og vurderingene må dokumenteres, f.eks. i et vedlegg til risikoanalysen. Når flere revisjoner er foretatt eller forutsetningene er radikalt endret, f.eks. ved store endringer i infrastrukturen, kan det være mest fornuftig å foreta en helt ny risikoanalyse.

En risikoanalyse vil ikke gi presise svar fordi det er knyttet usikkerhet til både sannsynligheter, konsekvenser og kostnader. Det er derfor viktig å være klar over at de alltid er knyttet usikkerhet til resultatene fra en risikoanalyse.

BS 7799 og risikoanalyse

BS 7799 er en britisk standard for etablering og håndtering av informasjonssikkerhet i organisasjoner. Standarden benyttes i flere land i Europa, og den vil også tjene som utgangspunkt for en norsk ordning for sertifisering av informasjonssikkerhet i organisasjoner. Standarden ble første gang publisert som britisk standard i 1995, og gjeldende utgave er fra 1999. Standarden er todelt, hvor del 1 gir anbefalinger og retningslinjer, mens del 2 setter krav til håndteringen av informasjonssikkerheten og oppbygningen av et ledelsessystem for informasjonssikkerhet.

Del 1 av standarden tar for seg 127 ulike anbefalinger/retningslinjer gruppert under 10 hovedområder:

- Sikkerhetspolicy
- Sikkerhetsorganisasjon
- Klassifisering av, og tilgang til, informasjon
- Personellsikkerhet
- Fysisk sikkerhet
- Systemdrift og kommunikasjon
- Adgangskontroll
- Systemutvikling og vedlikehold
- Beredskapsplanlegging
- Oppfølging av krav (lovverk osv.)

Del 2 av standarden spesifiserer oppbygningen av et ledelsessystem for informasjonssikkerhet, og setter krav til etableringen, vedlikeholdet og dokumenteringen av informasjonssikkerheten. Standarden beskriver seks trinn som må tas for å etablere dette systemet:

- Definerer av sikkerhetspolicy
- Bestemme hvilke deler av organisasjonen som skal inngå i systemet
- Gjennomføre risikoanalyse
- Håndtere risiko

- Velge ut hvilke elementer av BS 7799 del 1 som er relevante for organisasjonen
- Begrunne valgene gjort i foregående trinn

Etter at organisasjonen har etablert et rammeverk, må de utvalgte områdene fra del 1 implementeres i organisasjonen gjennom rutiner, tekniske løsninger osv. Deretter må det implementeres en kontinuerlig prosess med jevnlig internkontroller og ledelsesgjennomgang, slik at valgt strategi og løsninger stadig tilpasses skiftende teknologi og organisasjonens rammebetingelser.

Krav til risikoanalyse i BS7799

Som det framkommer av diskusjonen ovenfor stilles det i del 2 av BS7799 krav til at organisasjonen utfører en risikoanalyse. Hovedhensikten med denne er å balansere sikkerhetskravene, som kan hentes fra del 1, mot organisasjonens antatte trusselbilde. BS7799 beskriver risikoanalyse som en systematisk overveiing av a) sannsynlige skader som kan komme som et resultat av et sikkerhetsbrudd, når man vurderer potensielle konsekvenser av tap av konfidensialitet, integritet eller tilgjengelighet til informasjonen og andre verdier, og b) den realistiske sannsynligheten for at en slik feil skal skje sett i lys av fremtredende trusler og svakheter og eksisterende mottiltak. Standarden setter ikke spesielle krav til hvordan risikoanalysen skal utføres, men det eksisterer en veiledning til standarden, "PD 3002 – Risk assessment and risk management".

BS 7799 del 1 gir en rekke anbefalinger for sikkerhetstiltak en organisasjon bør implementere. Disse tiltakene har sin bakgrunn i kjente svakheter som kan unngås ved å innføre tiltakene. For eksempel er anbefalingen om å lage en fortegnelse over alle verdiene grunnet i en ide om at det å ikke ha en slik fortegnelse er en svakhet som kan føre til at organisasjonen ikke vet hva den skal beskytte og hvilke konsekvenser manglende beskyttelse kan ha. Ved å gjøre slike betraktninger for alle elementene i standarden har man en god oversikt over potensielle svakheter i organisasjonen og dermed et godt utgangspunkt for å utføre risikoanalysen.

Kritisk vurdering – hypoteser og usikkerhet

Kapittel

6

En risikoanalyse er en *hypotese* om sammenhenger, det er svært sjelden at den egentlig kan bevises eller ”valideres”. Det nærmeste vi kan komme er at et alvorlig sikkerhetsbrudd ”beviser” at gjeldende risikoanalyse var for dårlig.

Hypoteser - det være seg andres eller egne – innebærer alltid en usikkerhet. Erkjennelsen av dette ligger nok bak Datatilsynets råd (Veiledning i Risikoanalyse) om å ikke gå altfor ”vitenskapelig” til verks, og ikke operere med ”fine” tallfestinger. Av samme grunn er KITHs metodikk presentert i denne rapporten rimelig ”enkel”. Det finnes selvfølgelig mange mer sofistikerte metoder og tilhørende (kostbare) IT-verktøy. Faren er at metoden og verktøyet kan overskygge problemstillingen. Det er derfor best å starte med et enkelt oppsett som krever enkle hjelpemidler, og så bli mer sofistikert etter hvert.

Når utgangspunktet er at hypotesene er mangelfulle og usikre, må det være en løpende utfordring å være på utkikk etter *bekreftelser*, men også *avkreftelser* på at hypotesene som man bygger sikkerheten på er noenlunde riktige. Et godt avvikssystem er den fremste kilden til informasjon som kan brukes til å bekrefte eller avkrefte. Slik informasjon kan brukes til å forfine analysene, f.eks til å øke presisjonen og påliteligheten i dem. Men vær også oppmerksom på fallgrubene; det hører med til vår menneskelige natur at organisasjoner er mer tilbøyelige til å søke bekreftelse på sine antagelser, enn det motsatte. Når mye (annet enn sikkerhet) står på spill, øker sannsynligheten for at organisasjonen og enkeltindivider begår den feilen som kan kalles ”normalisering av avvik”. Dvs at vi (ubevisst) feiltolker og ”modifiserer” avvik slik at de (likevel) kan forklares i lys av rådende hypoteser, og på bakgrunn av dette legges i skuffen. På denne måten undertrykkes mulig kunnskap om latente og alvorlige svakheter i sikkerhetsbyggverket, inntil det en dag ”smeller” – og da gjerne ekstra kraftig fordi man er nesten uforberedt. Et åpent og søkende klima omkring avviksrapportering og –håndtering er derfor en god forsikring mot dette. En åpen og tillitsfull praksis omkring håndtering av avvik er følgelig noe av det mest sentrale og virkningsfulle i hele sikkerhetsarbeidet.

En risikoanalyse er altså aldri helt ”objektiv” i egentlig forstand, det er alltid en *subjektivitet* knyttet både til valg av analyseobjekter og til selve risikovurderingen. Men, den må aldri få preg av å være et skalkeskjul for en forhåndsgitt konklusjon. På den annen side bør man heller ikke bli skuffet over at tilsynsmyndigheter eller andre kontrollorganer ikke

ukritisk aksepterer selv den mest ”objektive” analyse. Det faktum at analysene aldri kan bli 100% objektive gjør det *ikke* lettere for andre å overprøve en lokal vurdering!

Seriøse risikoanalyser er altså effektive bidrag i arbeidet med å forbedre sikkerheten. Det er i utgangspunktet ingen grunn til at en organisasjon skal stole mer på andre enn på seg selv på dette området. Bruk derfor risikoanalyser til å analysere situasjonen, til å velge løsninger, til å dokumentere og til *argumentere* og stå for de valg dere gjør. Men, vær hele tiden åpen for at ”virkeligheten kan overgå fantasien”.

Referanser

Datatilsynet (1998), *Veiledning i risikoanalyse av informasjonssystem*

Næringslivets sikkerhetsorganisasjon (1998), *Faghefte 3, Risikoanalyse*

Direktoratet for sivilt beredskap (1998), *Risiko og sårbarhetsanalyser i arbeidet med år 2000-problematikken*

Direktoratet for sivilt beredskap (1994), *Veileder for kommunale risiko- og sårbarhetsanalyser*

Forsvarets Overkommando/Sikkerhetsstaben (1998), *Datasikkerhetsdirektivet, Direktiv for sikring av datasystemer gradert etter Sikkerhetsinstruksen eller Beskyttelsesinstruksen*

Risikoskjema



Hendelse/trussel:		Nr.
KONSEKVENSVURDERING		
Beskrivelse:		
Eksisterende skadebegrensende tiltak:		
		Katastrofal
		Kritisk
		Noen fare
		Ufarlig
SANNSYNLIGHETSVURDERING		
Årsaker:		
		Meget sannsynlig
Eksisterende forebyggende tiltak:		Sannsynlig
		Noe sannsynlig
		Lite sannsynlig
RISIKOVURDERING:		
Risikoreduserende tiltak:		
Forebyggende:		
Skadebøtende:		
Dato:	Utført av:	

HENDELSE/TRUSSEL:		Nr. 1.	
ÅRSAKER			
KONSEKVENSER			
EKSISTERENDE TILTAK			
SANNSYNLIGHETSVURDERING		KONSEKVENSVURDERING	
		Konf.	Int.
		Tilg.	
	Meget sannsynlig		Katastrofal
	Sannsynlig		Kritisk
	Noe sannsynlig		Noen fare
	Lite sannsynlig		Ufarlig
RISIKOVURDERING			
RISIKOREDUSERENDE TILTAK			
Dato:		Utført av:	

