22. juli-kommisjonen

NOTAT: 8 /12

RISIKOBASERT SIKRING (SECURITY) OG RISIKOREDUKSJON

Morten Bremer Mærli
Forsker
Det Norske Veritas

08.03.2012

www.22julikommisjonen.no

DET NORSKE VERITAS

Risikobasert sikring (security) og risikoreduksjon

Notat til 22. Juli-kommisjonen

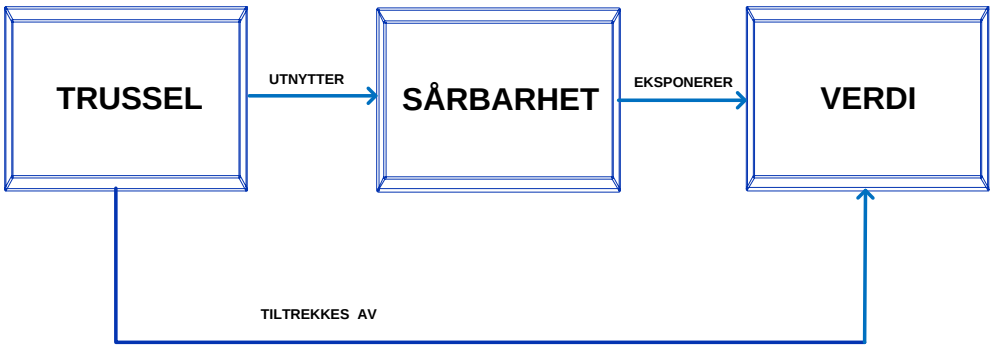
Notat: Risikobasert sikring (security) og risikoreduksjon		DET NORSKE VERITAS AS **1322 Høvik**, **Norway** Tlf: **+47 67 57 99 00** Faks: **+47 67 57 99 11** http://www.dnv.com Org. nr: NO 945 748 931 MVA
Kunde:	22. juli-kommisjonen	
Kontaktperson:	Bjørn Otto Sverdrup	
Utarbeidet av: Morten Bremer Mærli	*Verifisert av:* Henrik Fonahn Rolf Lervik	*Godkjent av:* Erling Svendby

INTRODUKSJON

I det følgende gis noen betraktinger om risiko knyttet til tilsiktede uønskede handlinger – eller "security" i engelsk terminologi. Dokumentet bygger på analysemetodikk utviklet av DNV og er kompatibelt med relevante nasjonale og internasjonale standarder.

RISIKO

Sikringstiltak mot ulike farer har vært sentralt i alle samfunn, i all tid. Manglende eller utilstrekkelig beskyttelse innebærer sårbarheter som kan eksponere verdier eller annet som ønskes sikret. Eiere av verdiene står overfor risiko for verditap eller direkte og indirekte skade. Denne risikoen kan uttrykkes som forholdet mellom trusselen mot en gitt verdi og verdiens sårbarhet overfor trusselen. Dette er illustrert i Figur 1.



Figur 1. Risiko som en trussel som utnytter en sårbarhet som eksponerer en verdi.

Sårbarhet kan forstås som forhold som reduserer eller begrenser evnen til å motstå aksjoner mot mål hvor verdiene finnes. Eksempler spenner fra ulåste dører til utro tjenere (såkalte *insidere*). Verdier kan være både materielle og immaterielle. Eksempler på immaterielle verdier er en virksomhets omdømme eller velfungerende, samfunnskritiske funksjoner.

Trusselen bestemmes av hvem som ønsker å oppnå hva, med hvilke midler og med hvilke mål. Faktiske trusler oppstår ikke før "noen" har både vilje og evne til å gjennomføre et anslag. Skaper ikke verdiene interesse er risikoen neglisjerbar. Tilsvarende kommer selv dedikerte angripere ingen vei uten nødvendige kapasiteter.

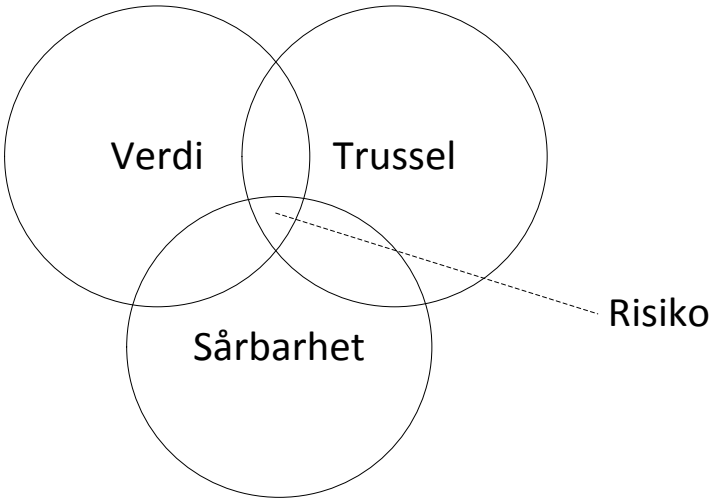
Hvorfor og i hvilken grad trusselaktører tiltrekkes av verdiene avhenger av egenskaper ved verdiene, i kombinasjon med aktørenes intensjoner. Er terrorister på banen, vil typisk verdier med stort og markant skadepotensiale være attraktive mål. Tyver vil typisk se på vinningspotensialer, som også (industri)spioner gjør. Men mens vanlige kriminelle er ute etter verdisaker, er informasjon målet for spionen.

Mål som fra utsiden synes svært godt beskyttet, kan framstå som mindre attraktive enn dårlig sikrede mål. Større verdier kan øke trusselaktørenes risikovillighet. Men angrepsviljen er avhengig av deres egne antakelser om sine evner i møte med sikringstiltak ved utvalgte mål, samt andre utfordringer de kan forutse. Summen av slike antakelser vil bestemme et måls attraktivitet, og dermed sannsynligheten for at målet angripes.

Fordi handlingen er gjennomført med vilje, gir dette dessuten trusselaktørene mulighet til å påvirke utfallet (konsekvensene). Valg av tid og sted for aksjonen vil spille inn i forhold til hvem og hvor mange som rammes. Gjerningsmenn kan dessuten introdusere barrierer som hindrer skikkelig respons.

RISIKOREDUKSJON

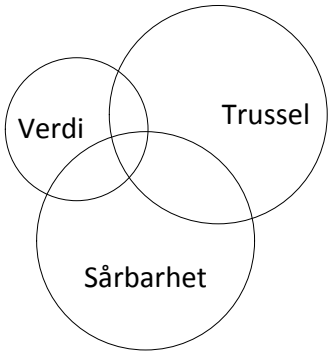
Risiko oppstår altså i samspillet mellom verdier, trusler og sårbarheter; fjernes verdiene, fjernes også risikoen. Uten trussel kan sårbarheten godt være stor, uten at dette påvirker risikoen. Tilsvarende vil verdiene være sikre(t) dersom det – i teorien – ikke finnes sårbarheter. Figur 2 illustrerer.



Figur 2. Risiko, verdi, trussel og sårbarhet

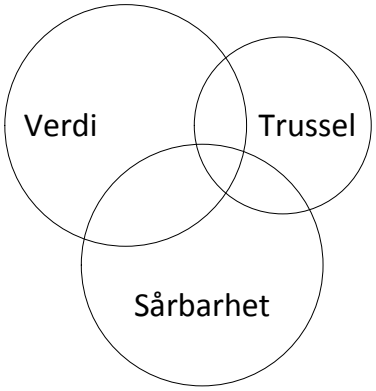
Risikoen for tap av kritiske objekter og eller verdier kan følgelig reduseres på tre måter: Trusselen kan motvirkes direkte, sårbarheter i sikringen kan identifiseres og elimineres, eller verdier og objekter kan fjernes, flyttes eller konsolideres. En sunn sikringspraksis bør vurdere, og eventuelt inkludere, alle elementene, men i varierende grad.

Verdireduksjon



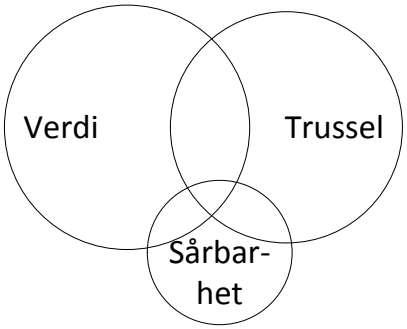
Verdier kan konsolideres for å redusere sikringskostnader, men generelt har verdireduksjon iboende begrensninger. Verdier er, i vid forstand, verdifulle. De er som oftest der for en grunn. En sikringsstrategi kan være å redusere verdien av verdier som kompromitteres eller stjeles, - verdier som eieren altså mister kontrollen over. Både bruksverdien av sedler som er blitt farget i forbindelse med ran, og nytteverdien av stjålne, krypterte harddisker kan være begrenset. I begge tilfeller er målsetningen å gjøre verdiene mindre attraktive.

Trusselreduksjon



Overvåkning kan gi viktige indikasjoner på forestående angrep eller på spesielt utsatte næringer. Men ofte blir ikke trusler oppdaget før det er for sent. Tradisjonelle trendanalyser kan ha begrenset relevans dersom gjerningsmennenes vilje og evne til innovasjon er stor. Og, eventuell intervensjon mot identifiserte trusler kan generere nye trusler – et velkjent problem innen terrorbekjempelse. Generelt er trusselkomponenten den vanskeligste og den mest usikre delen av risikovurderinger.

Sårbarhetsreduksjon



Hva da med sårbarheter? Sårbarheter vil alltid være tilstede. Som for trusler, er også disse krevende å hanskes med. Men som for verdier, eier den enkelte virksomhet sine egne sårbarheter og har mulighet til å gjøre noe med disse. Tettes én sårbarhet, kan dette i mange tilfeller stoppe flere trusler. Trusselspesifikke scenarioer gjør det mulig å analysere eksisterende kontroller (organisatoriske og fysiske), samt kartlegge sårbarheter ved virksomheten. Ved å koble trusselaktørenes motiver til objekter, og deres kapasitet mot hvor godt verdiene er sikret, er grunnlaget for risikobaserte, kostnadseffektive sikringsløsninger lagt.

RISIKOBASERTE TILTAK

Kjente risikoer trigger gjerne tiltak, eller interesse for tiltak, for å redusere risikoen (og usikkerheten). Utfordringen ligger selvsagt i å treffe rett – å sette inn de riktige tiltakene, til rett tid, på rett måte. Der det lenge har handlet om tykke vegger og massiv beskyttelse av businesskritiske objekter og verdier, handler det i dag i større grad om å tilpasse sikringen til truslene. Her har strukturerte, kunnskapsbaserte sikringsløsninger og klar ledelse av sikringsinnsatsen vist seg å gi god uttelling, også økonomisk.

Men altfor ofte mangler virksomheter skikkelig oversikt over hva de har av verdier, informasjon eller prosesser som krever beskyttelse. Det er et dårlig utgangspunkt for sikring, og sårbarhetene kan lett bli større enn hva både kjent og godt er. Uansett, gjennomtenkte prioriteringer må på plass: Alt kan ikke sikres like godt, hele tiden. Sikring for sikringens skyld er heller ikke av det gode. Deteksjon- og barriersystemer installeres i så fall fra en "kjekt-å-ha"-tankegang, uten skikkelig forståelse av hva sikringen skal beskytte, hvorfor, mot hvem og hvordan. Konsekvensen kan bli dyre utstyrsløsninger, og dyrekjøpte erfaringer.

For enkelte handler sikring og beskyttelse likevel i stor grad om "Guns, Guards, Gates" – med andre ord fysiske, synlige tiltak. Slike tiltak er nødvendige, men ikke tilstrekkelige. Eksempelvis dreier det seg ikke bare om antall kameraer, eller hvor disse er plassert. Typisk vil også prosedyrer, trening, vedlikehold og rådende organisasjonskultur være faktorer som bestemmer hvor effektivt et sikringsregime er. Selv små organisatoriske justeringer kan bety mye for sikringen i praksis.

Sikring skapes gjennom daglig virke og vaktsomhet, i samspillet mellom organisasjon, menneske og teknologi. Roller må være klart definert med ansvar, myndighet og oppgaver, og dette må være kommunisert og forstått av den enkelte. Et ledelsessystem for sikring skal være et rammeverk for å sikre at risiko blir identifisert, og for at tiltak blir definert, implementert og fulgt opp. Slike systemer må følgelig integreres som en naturlig del av virksomhetens øvrige styringsprosesser og ledelsessystem.

KONKLUSJON

Sikring handler først og fremst om forebygging. Men sikring er mer enn å følge regler. I et godt, velfungerende sikringsregime er helheten større enn summen av de enkelte delene. Sikring skapes, daglig, gjennom virke og vaktsomhet, av alle i organisasjonen. Sikring handler om å kommunisere ansvar og om myndiggjøring. Ledelse, utvikling av en god sikringskultur, ansvarliggjøring og ressursprioriteringer er nødvendig for å oppnå god og vedvarende sikring i praksis.

I en sikringskontekst, kan forståelse av sårbarheter være spesielt viktig. Der trusler er usikre og svingende, kan sårbarheter – dersom de identifiseres – være nøkkelen til kostnadseffektiv risikoreduksjon. Det er krevende å betale for at noe ikke skal skje, til mange sikkerhetsansvarliges daglige frustrasjon. En viktig erkjennelse er, paradoksalt nok, at sikring synes best når den feiler eller utfordres. Og kanskje er det derfor trenden fremdeles er krise- og beredskapsøvelser, snarere enn sikringsøvelser, som motsats til tiltak som primært forsøker å respondere når skaden allerede har skjedd.

Det Norske Veritas:

Det Norske Veritas (DNV) is a leading, independent provider of services for managing risk with a global presence and a network of 300 offices in 100 different countries. DNV's objective is to safeguard life, property and the environment.

DNV assists its customers in managing risk by providing three categories of service: classification, certification and consultancy. Since establishment as an independent foundation in 1864, DNV has become an internationally recognised provider of technical and managerial consultancy services and one of the world's leading classification societies. This means continuously developing new approaches to health, safety, quality and environmental management, so businesses can run smoothly in a world full of surprises.

Global impact for a safe and sustainable future:

Learn more on www.dnv.com

Kommisjonen og sekretariatet er i dialog med en rekke eksterne eksperter som et ledd i sin undersøkelse og utredning. Notatene er utarbeidet av eksterne eksperter etter ønske fra kommisjonen. Notatene er ikke i seg selv et resultat av kommisjonens eller sekretariatets arbeid og bør ikke på noen måte oppfattes som offisielle eller uoffisielle observasjoner, meninger eller anbefalinger fra kommisjonen. Alle observasjoner, meninger og anbefalinger fremsatt i disse notatene er utelukkende forfatternes.