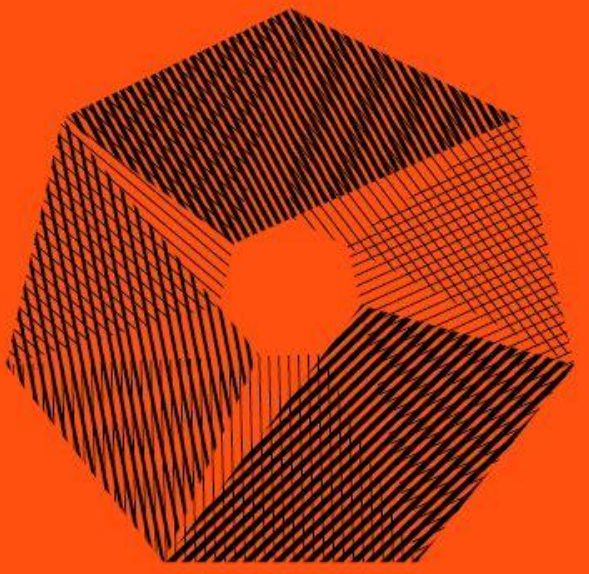

BESLUTNINGER OM SIKKERHET

– en praktisk guide

Teknologirådet

BESLUTNINGER OM SIKKERHET – EN PRAKTISK GUIDE

ISBN 978-82-92447-58-1 (trykket utgave)
ISBN 978-82-92447-59-8 (elektronisk utgave)
Utgitt: Oslo, april 2013
Omslag: Commando Group
Elektronisk publisert på: www.teknologiradet.no

BESLUTNINGER OM SIKKERHET – EN PRAKTISK GUIDE

I årene etter angrepet på USA 11. september 2001, opplevde verden flere store terroranslag. Angrepene mot Madrid i 2004 og London i 2005 førte til at sikkerhet og teknologi virkelig ble satt på agendaen i Europa. Først og fremst fordi man så en voldsom investering i sikkerhetsteknologi, først på flyplasser og senere i store deler av samfunnet. Men også fordi disse investeringene førte til diskusjoner om hvilke samfunnsmessige verdier som ble satt på prøve av den nye teknologien. Mange av disse investeringene har i etterkant blitt sett på som mindre vellykkede, da de negative konsekvensene for samfunnet har blitt større enn den tiltenkte økningen i sikkerhet. Et eksempel er forsøket på å innføre de såkalte «nakenskannerne» på norske flyplasser i 2007. For å bedre sikkerheten på norske flyplasser ønsket luftfartsmyndighetene å innføre skannerne i sikkerhetskontrollen. Etter en pilotperiode på Sola lufthavn ble prosjektet avsluttet. Store protester fra de ansatte, publikum og fagforeninger gjorde at prosjektet ikke lot seg gjennomføre som planlagt.

Slike problemer kan oppstå når beslutningstakerne ikke tar høyde for de mange ulike situasjonene investeringen kommer til å bli en del av ute i samfunnet. Beslutninger rundt ulike sikkerhetsløsninger har tidligere stort sett vært basert på økonomiske vurderinger og et mål om økt sikkerhet. Det er på tide at sikkerhetsløsninger blir vurdert på et mye bredere grunnlag, slik at vi får et trygt samfunn, men samtidig tar hensyn til et bredere spekter av samfunnets verdier.

I Norge har hendelsene 22. juli 2011 satt fokus på sikkerhet og beredskap i samfunnet, og vi vil trolig se en økning i sikkerhetsinvesteringer, både i det private og offentlige. Hva kan vi gjøre for at disse investeringene skal fungere

på best mulig måte i samfunnet? Hvem skal involveres når slike beslutninger skal tas? Hvordan kan man gå frem for å kunne ta gode beslutninger?

DESSI-METODEN

DESSI (Decision Support on Security Investment) er en prosess for beslutningsstøtte som tar hensyn til kompleksiteten i dagens samfunn og gir et bud på hvordan man kan håndtere dette i praksis. Prosessen åpner opp beslutningsrommet, henter innspill fra flere aktører og tar inn flere perspektiver i beslutningsprosessen.

Hovedtanken bak DESSI er at beslutninger om sikkerhet må vurderes i et bredere samfunnsmessig perspektiv enn det som har vært vanlig. Prosjektet har definert syv dimensjoner det er viktig å ta hensyn til når man skal innføre en sikkerhetsløsning. Ved å vurdere de ulike løsningsalternativene mot disse dimensjonene får man en bredere forståelse av både de positive og negative effektene løsningen kan ha på samfunnet. Dette gir grunnlag for en mer robust prosess og gir forbedret mulighet for at løsningen vil fungere godt i samfunnet når den blir implementert.

DESSI er utviklet av et prosjektkonsortium med partnere fra Norge, Danmark, Østerrike og Tyskland og er finansiert gjennom EUs 7. rammeprogram[1]. Teknologirådet har vært partner i prosjektet som avsluttes i 2013.

Høsten 2012 og våren 2013 har DESSI-prosessen blitt testet i flere europeiske land. I Østerrike har man vurdert nye sikkerhetstiltak i rettsbygninger gjennom et DESSI-prosjekt. I Danmark ble DESSI testet sammen med et busselskap som forsøker å finne den beste måten å beskytte sine sjåfører mot angrep.

I forbindelse med testing av prosessen og formidling til norske aktører, har Teknologirådet bearbeidet og oversatt metoden til norsk og norske forhold. Gjennom et samarbeid med Røde Kors har DESSI og Teknologirådet vurdert om droner kan være et godt verktøy for å gjennomføre tryggere og mer effektive søk- og redningsoperasjoner i Norge.

[1] Mer informasjon på www.securitydecisions.org

EN PROSESS FOR ROBUSTE BESLUTNINGER

DESSI har utviklet en fleksibel prosess som involverer et bredt spekter av metoder og aktører. Målet er å få flere perspektiver med i diskusjonen, både når det gjelder selve sikkerhetsutfordringen og de ulike løsningsalternativene.

Prosessen er delt i tre faser:

1: Beskrivelse av sikkerhetsutfordringen
2: Identifisere og beskrive løsningsalternativene
3: Vurdere løsningsalternativene opp mot DESSIs dimensjoner

De tre fasene gjennomføres som arbeidsmøter eller workshops, og man kan selv velge i hvor stor grad man ønsker å involvere eksterne deltakere. Målet når man velger deltakere er å få inn flere perspektiver både når det gjelder sikkerhetsutfordringen og løsningsalternativene. Prosessen kan gjennomføres på egenhånd – eller ved hjelp av et nettbasert verktøy, utviklet i DESSI prosjektet.

FASE 1: SIKKERHETSUTFORDRINGEN

I den første fasen av DESSI beskrives sikkerhetsutfordringen så nøyaktig som mulig, slik at man får oversikt over hvilke behov en mulig investering må dekke og hvilke grupper som er eller kan bli påvirket av utfordringen og de mulige løsningsalternativene.

Formålet med å lage en beskrivelse av utfordringen, er å skape refleksjon rundt situasjonen og å oppnå en bredere forståelse av utfordringen man står overfor. I tillegg kan denne beskrivelse brukes senere i prosessen for å informere eksterne prosessdeltakere om sikkerhetsutfordringen.

Fase 1 gjennomføres av personer i organisasjonen som sammen skriver et notat om sikkerhetsutfordringen.

> ***Eksempel på sikkerhetsutfordring:*** *Røde Kors i Norge ønsket å undersøke i hvilken grad nye typer teknologi kunne bidra til å øke personsikkerhet og effektivitet i søkeaksjoner. Aksjonene foregår ofte i ulendt og til tider farlig terreng (for eksempel etter snøskred), og Røde Kors ønsket å utforske løsninger som kan lette og sikre dette arbeidet. Hovedutfordringen ble formulert som en søkeaksjon etter savnet person i ulendt skogs- og/eller fjellterreng. Utfordringen inkluderte også scenarier om ulike værforhold.*

VEILEDENDE SPØRSMÅL

Hva er sikkerhetsutfordringen som skal løses av deg/din organisasjon?

Hvem eller hva er det som skaper utfordringen?

Hvem eller hva skal beskyttes gjennom å implementere en løsning?

Hva slags skade kan utfordringen føre til? (økonomisk, fare for liv og helse, skade på infrastruktur, symbolsk skade e.l.)

Har utfordringen eksistert over lengre tid, eller har den oppstått på grunn av en spesifikk hendelse?

Har dere prøvd å løse utfordringen tidligere? Hvis ja, hvordan og med hvilket resultat?

FASE 2: LØSNINGSALTERNATIVER

I den andre fasen av prosessen finner man mulige løsningsalternativer på sikkerhetsutfordringen. Dette kan være flere alternative løsninger, eller man kan beskrive en enkelt løsning.

Hvis ønskelig kan man involvere eksterne sikkerhetseksperter som kan komme med forslag til mulige løsninger etter å ha lest beskrivelsen av sikkerhetsutfordringen.

Fasen gjennomføres som en workshop hvor man kan invitere internt i organisasjonen og eksterne sikkerhetseksperter. Etter en introduksjon av sikkerhetsutfordringen deles deltakerne i grupper som diskuterer ulike løsninger de tror kan fungere.

Gruppene presenterer så sine alternativer i plenum, og gjennom en felles brainstorm prøver man å sortere, slå sammen og spesifiserer alternativene – til man kommer frem til de mest relevante som tas med videre i prosjektet

Mot slutten av denne fasen velger man de mest relevante alternativene, som vil bli videre vurdert i fase tre.

> ***Eksempel på løsningsalternativer:*** *Domstolen i Østerrike har over lengre tid opplevd angrep på ansatte i forbindelse med saker knyttet til familierett. De arrangerte en workshop for å identifisere ulike løsningsalternativer på denne sikkerhetsutfordringen. De inviterte ansatte, dommere, sikkerhetseksperter og arkitekter for å diskutere seg frem til ulike alternativer. Løsninger som ble foreslått varierte fra en mer åpen arkitektur og sikkerhetskontroll ved inngangen, til et servicesenter som sørger for god mottakelse av de besøkende.*
>
> *I Danmark ble DESSI testet sammen med et busselskap som opplevde hærverk og trakassering av sine sjåfører. Fase 2 ble gjennomført med bussjåfører, sikkerhetseksperter, representanter fra fagforeninger, arbeidstilsynet og det kriminalpreventive råd. De to løsningene man satt igjen med etter workshopen var forslag om en vegg av plexiglass mellom sjåføren og passasjerene, og tilbud om stress- og konflikthåndteringskurs for de ansatte i busselskapet.*

VEILEDENDE SPØRSMÅL

Hva slags type løsning er dette? (juridisk, teknologisk, organisatorisk e.l.)

Hva slags effekter er forventet ved denne løsningen? (både positive og negative)

Hvor skal løsningen implementeres? (fysisk hos organisasjonen, ute i samfunnet, i et datasystem e.l.)

Når kan løsningen implementeres og når kan man forvente effekter? (umiddelbart, kort tidshorisont, lengre tidshorisont) Har løsningen en begrenset levetid?

Hva er kostnadene for innkjøp, implementering og drift av løsningen?

FASE 3: VURDERING AV ALTERNATIVER

I denne siste fasen vurderes løsningsalternativene opp mot DESSIs samfunnsdimensjoner og kriterier. Dimensjonene er kort beskrevet med en introduksjonstekst hvor kriteriene innenfor hver dimensjon er formulert som veiledende spørsmål. Hvis ønskelig kan man involvere eksterne eksperter som kan bidra med kunnskap om dimensjonene, og hvordan løsningsalternativene kan virke i disse.

Fase 3 gjennomføres som en workshop hvor man kan involvere deltakere internt i organisasjonen og eksterne eksperter. Deltakerne deles inn i grupper som skal ta for seg en eller flere dimensjoner og vurdere hvordan løsningsalternativene fungerer i disse. Hvis man mangler ekspertise på noen områder i organisasjonen kan det være en god idé å invitere for eksempel en jurist som kan bidra med ekspertise om den juridiske dimensjonen eller en ekspert som kan hjelpe til med vurderinger om økonomiske forhold.

Etter at gruppene har diskutert samles man til en plenumsdel hvor hovedpunktene fra gruppediskusjonene presenteres. Hvis man har forslag til hvordan løsningsalternativene kan justeres og gjøres bedre kan disse løftes frem i denne delen.

Resultatet av denne siste fasen vil ikke være en rangert liste over løsningsalternativer, men man får en fyldig beskrivelse av hvordan de ulike løsningene vil fungere i dimensjonene. Deretter må man selv bestemme hvilken løsning som er det beste for sin organisasjon. Avgjørelsen bygges nå på et bredt samfunnsmessig grunnlag, hvor flere aktører har fått delta i vurderingene.

En mer utførlig beskrivelse av dimensjonene og veiledende spørsmål finnes i neste kapittel.

> ***Eksempel på vurdering:*** *Røde Kors sin utfordring rundt søk- og redningsaksjoner ble diskutert på en workshop i Oslo. Deltakere var fra flere lokallag i Røde Kors, den norske bransjeforeningen for droner, eksperter innen sikkerhet og beredskap, personvern, etikk og økonomi.*

Etter en kort introduksjon til sikkerhetsutfordringen og de to løsningsalternativene ble deltakerne delt i grupper. Hver gruppe diskuterte begge alternativene opp mot en spesifikk dimensjon. Etter gruppediskusjonene møttes man i en plenumssesjon hvor man diskuterte hvordan alternativene hadde blitt vurdert i gruppene.

DIMENSJONER OG KRITERIER

Det viktigste elementet i DESSI-metoden er å vurdere potensielle løsninger opp mot flere samfunnsdimensjoner enn det som har vært vanlig. Tidligere har det overordnede målet om økt sikkerhet innenfor en gitt økonomisk ramme, overskygget andre aspekter ved investeringer i sikkerhetsløsninger. For å åpne opp beslutningsprosessen har DESSI definert syv dimensjoner som spenner fra økonomi og lovverk til samfunnsmessige og politiske forhold. Dimensjonene som er valgt, dekker de områder som oftest influeres av mulige sikkerhetsløsninger og er grundig definert i DESSI prosjektets rapporter «Dimensions in Security Investment[2]» og «System of Criteria[3]».

Gjennom å vurdere ulike løsninger mot de syv dimensjonene får man et bredere og mer robust beslutningsgrunnlag.

1: ØKT ELLER REDUSERT SIKKERHET

Sikkerhet kan defineres som fravær av fare – det vil si en situasjon hvor den ønskede tilstanden ikke er truet eller forstyrret på noen måte. Man kan lage et skille mellom objektiv og subjektiv sikkerhet. Med objektiv sikkerhet menes sannsynligheten for fare, mens subjektiv sikkerhet refererer til en trygghetsfølelse eller fravær av frykt.

Sikkerhet er et konsept som kan være vanskelig å måle. For å finne ut om et tiltak har hatt en effekt kan man prøve å identifisere en forandring. Denne

[2] http://securitydecisions.org/download/8/
[3] http://securitydecisions.org/download/9/

forandringen kan være fysisk (ved at et tiltak har forandret de fysiske omgivelsene), psykisk (menneskene involvert føler seg tryggere) eller diskursiv (for eksempel at en diskusjon i media om sikkerhetsutfordringen roes ned etter at tiltaket er innført). Sikkerhetstiltak kan påvirke aktører på ulike måter. Derfor er det viktig å ha i bakhodet at det som øker sikkerheten for noen, kan gjøre andre mer utrygge.

VEILEDENDE SPØRSMÅL

Er det mulig å måle en eventuell økning av sikkerheten? Vil løsningsalternativet opprettholde tingenes tilstand, eller føre til en forandring?

Hvem vil påvirkes av løsningen? Vil dette alternativet føre til økt trygghetsfølelse for noen, men en redusert trygghetsfølelse for andre?

Sikkerhetsteknologi blir noen ganger innført uten at det har vært et angrep eller en hendelse. Er løsningen tenkt som et forebyggende tiltak?

Blir løsningen vurdert på grunn av offentlig debatt eller etterspørsel, eller på grunn av en reel trussel?

2: MENNESKERETTIGHETER OG ETIKK

Bruk av sikkerhetsteknologi kan føre til økt inngripen i individuelle rettigheter og etiske normer. Mens grunnleggende rettigheter er forankret i et juridisk lovverk, er etikk mer dynamisk, kultur- og kontekstavhengig. Etiske normer kan forandre seg over tid, og nye etiske betraktninger kan gjøre seg gjeldene ettersom samfunnet utvikler seg. Grunnleggende rettigheter og etiske aspekter er svært viktig med hensyn til ny sikkerhetsteknologi, ikke minst fordi disse kan være en del av ømtålige problemstillinger i en samfunnsdebatt.

En generell utfordring når det kommer til forholdet mellom sikkerhetstiltak, grunnleggende rettigheter og individer, er at gjennomsnittspersonen ikke nødvendigvis er klar over egne rettigheter og hva de innebærer. Hvis de heller ikke har informasjon om hvor og hvordan sikkerhetsteknologi virker i samfunnet er det vanskelig å reagere på etiske og juridiske avvik.

VEILEDENDE SPØRSMÅL

Tar løsningen hensyn til retten til privatliv, personvern og beskyttelse av personopplysninger?

Tar løsningen hensyn til ytrings- og informasjonsfrihet, samvittighets- og religionsfrihet?

Gir tiltaket rom for mangfold, likhet og verdipluralisme?

Kan løsningen virke diskriminerende for enkelte grupper av mennesker?

Er løsningen og dens virkninger enkle å forstå? Er det tilstrekkelig formidlet hva løsningen vil innebære for de som blir involvert eller påvirket?

Er løsningen hensiktsmessig, nødvendig og proporsjonal i forhold til sikkerhetsutfordringen?

3: LOVVERK

Debatten omkring rettslig regulering av sikkerhetsinvesteringer og -tiltak dekker et bredt spekter av problemstillinger. Den siste tiden er det særlig avveiningen mellom åpenhet og sikkerhet, som har fått mye oppmerksomhet. Hvor viktig er retten til respekt for privatliv og personvern, og i hvilken grad bør staten tillates å gripe inn i borgernes liv?

Mens en forbrytelse kan defineres som et lovbrudd etter at den er begått, er det vanskeligere å håndtere potensielle sikkerhetstrusler. Det er enklere å straffe en som har vært med på en terrorhandling, enn en som mistenkes å planlegge et fremtidig lovbrudd.

En annen utfordring er den hurtige teknologiutviklingen, og hvordan loven kan forholde seg til nye teknologier. Hva bør anses som brudd på grunnleggende rettigheter, og hvordan kan man opprettholde de prinsipper som gjelder i en rettstat, i møte med nye sikkerhetsteknologier?

VEILEDENDE SPØRSMÅL

Dersom løsningen innhenter, lagrer eller bruker personopplysninger, samsvarer den med loven om beskyttelse av personopplysninger?

Er det definert hvem som har ansvaret for funksjonalitet og/eller svikt i løsningen?

Er investeringen sikret mot misbruk? Kan løsningen sikres mot annen bruk enn den opprinnelig planlagte?

Er løsningen i overensstemmelse med arbeidsmiljøloven?

Er løsningen i overensstemmelse med naturvernlovgivning?

Dekker eksisterende lovverk bruk av eventuell ny teknologi som inngår i løsningen?

4: SOSIALE IMPLIKASJONER

Sikkerhetsløsninger kan ha følger for en rekke samfunnsmessige forhold, enten det påvirker den enkelte borger, organisasjoner, byer eller samfunnet som en helhet. Konsekvenser for individer kan ha en direkte og omgående effekt, mens det på samfunnsnivå kan være mer indirekte effekter som virker over tid. Derfor blir det viktig å se de samfunnsmessige forholdene i et bredt og langsiktig perspektiv når man vurderer løsningsalternativene.

VEILEDENDE SPØRSMÅL

Har løsningen negative konsekvenser for spesifikke yrkesgrupper, arbeidstakere eller selvstendige næringsdrivende?

Fører løsningen direkte eller indirekte til lik behandling av individer?

Oppfordrer løsningen til involvering fra utenforstående aktører når det gjelder styresett og ledelse?

Øker løsningen borgernes tilgang til deltakelse ved kulturelle eller sosiale begivenheter (for eksempel demonstrasjoner eller store kulturelle arrangementer)?

5: AKSEPT AV RISIKO

Når man planlegger å implementere en sikkerhetsløsning er det viktig å undersøke hvorvidt det er aksept for løsningen blant de individer eller grupper som vil bli påvirket. Aksept er viktig for at løsningen skal kunne fungere slik som planlagt. En eventuell risiko ved sikkerhetsutfordringen eller den planlagte løsningen bør kommuniseres til alle involverte parter.

Hvorvidt man aksepterer risiko eller ikke, kommer an på forholdet mellom idealet om absolutt sikkerhet, de behov løsningen skal møte og faktorer som effektivitet, bruksområde og økonomi. Dette forholdet kan påvirkes både av den samfunnsmessige og teknologiske utviklingen. Samtidig kan også enkelthendelser gjøre noe med hvordan man vurderer risiko. Ulykken ved kjernekraftverket i Fukushima i 2011, gjorde at mange endret oppfatning av risikoen forbundet med slike anlegg.

Dette gjør at man bør evaluere hva som er et akseptabelt risikonivå for hver enkelt sikkerhetsløsning. Noe som ble akseptert for ti år siden vil kanskje ikke bli akseptert i dag – eller omvendt.

VEILEDENDE SPØRSMÅL

Kan løsningen innføres uten å skape ny risiko?

Er det en god balanse mellom risikoen forbundet med sikkerhetsutfordringen og den planlagte løsningen?

Er løsningen ønsket av berørte personer? Er de berørte personene med i beslutningsprosessen?

Utsettes enkelte grupper for økt risiko? (for eksempel spesielt sårbare grupper, eller grupper som mangler kapasitet til å håndtere risiko)

Er det mulighet for at løsningen kan forårsake protester fra interesseorganisasjoner eller andre grupper?

6: DEMOKRATI

I møte med ønsket om økt sikkerhet kan tiltak ment å beskytte demokratiet, ende med å undergrave demokratiske kjerneverdier som likhet, politisk toleranse, åpenhet og rettssikkerhet.

Debatter omkring sikkerhetsinvesteringer kan avpolitiseres ved at borgere og beslutningstagere mister muligheten til å påvirke avgjørelser om sikkerhet. Ved å gjøre sikkerhet til et tema som krever ekspertkunnskap, undergraves borgernes forståelse og mulighet til å gjøre valg omkring innføringen av sikkerhetstiltak. Det er viktig å anerkjenne at vanlige borgere også har viktig kunnskap når det kommer til hvordan sikkerhetsløsninger fungerer i samfunnet.

VEILEDENDE SPØRSMÅL

Kan løsningen påvirke tillitsforholdet mellom stat og borger?

Kan løsningen føre til økt demokratisk deltakelse og fri meningsutveksling om sikkerhet og åpenhet?

Kan løsningen misbrukes politisk, til å kontrollere samfunnet eller enkelte grupper?

Fremmer løsningen en maktbalanse mellom eksperter og lekfolk?

7: ØKONOMI

Hvordan skal økt sikkerhet finansieres? Hvilke budsjetter bør økes og hvilke bør strammes inn? Statlige og offentlige institusjoner er viktige når det gjelder sikkerhetstiltak på samfunnsnivå – de legger føringer gjennom lovverk og styresett og er også en betydelig aktør når det kommer til etterspørsel av sikkerhetstjenester.

Mange private bedrifter er også viktige; både som tilbydere og kunder. Private aktører som er avgjørende for infrastruktur er særlig viktige, som strømleverandører, transportselskap og helseforetak.

For å kunne gjøre en sikkerhetsinvestering så forutsigbar som mulig er det viktig å ha informasjon om kostnader til innkjøp og implementering, men også til videre drift.

VEILEDENDE SPØRSMÅL

Vet man de de direkte kostnadene forbundet med løsninger? Kan man oppgi hva drift av løsningen vil koste?

Kan man oppgi indirekte kostnader og eventuelle uventede kostander forbundet med løsningen?

Kan løsningen stimulere til økt forskning og utvikling?

Kan løsningen ha positive makroøkonomiske virkninger?